Email: committeeservices@horsham.gov.uk
Direct line: 01403 215465

Horsham District Council

Scrutiny & Overview Committee
Business Improvement Working Group

Tuesday 13th October 2015 at 6.00pm
Lewes Room, Parkside, Chart Way, Horsham

Councillors: Brian O'Connell (Chairman
John Chidlow (Vice-Chairman) David Jenkins
Paul Clarke Godfrey Newman
Jonathan Dancer Michael Willett
Tony Hogben

You are summoned to the meeting to transact the following business

Tom Crowley
Chief Executive

Agenda

		Page No.
1.	Apologies for absence	
2.	To approve as correct the minutes of the meeting held on 28th July 2015 (attached)	3
3.	To receive any declarations of interest	
4.	Announcements from the Chairman or the Chief Executive	
5.	Business Transformation Programme, including office move: presentation from the Business Transformation Officer	
6.	Property & Asset Management Review: update from the Property & Facilities Manager (oral)	5
7.	Review of Working Group's work programme for 2015/16:	

- Property Development – Property & Asset Management Review following department restructure
- Review of the S106 Process
- Appeals process – policy and procedure review. To include planning process mapping exercise

Continued/…

8. To scope the Review of S106 arising from the Scrutiny & Overview Committee on 14th September

9. Annual Member Overview of Horsham District Council's Corporate Policy and Procedures Document on the Regulation of Investigatory Powers Act 2000 7

Terms of Reference for Business Improvement Working Group

- Scrutinise business improvement proposals focusing on the most significant in terms of benefit, effect upon services and risk
- Encourage consideration of best practice
- Monitor progress including post-implementation review
- Report findings in terms of benefits, effect upon services, risk and progress to Scrutiny
- To investigate other matters related to operational effectiveness and business improvement that the Scrutiny and Overview Committee or the Finance and Performance Working Group might request be investigated
- To liaise with other working groups to avoid duplication of activity

Notes of the Scrutiny and Overview Committee
Business Improvement Working Group
28th July 2015

Present: Councillors: John Chidlow, Godfrey Newman, Brian O'Connell, Michael Willett

Apologies: Councillors: Jonathan Dancer, Tony Hogben, David Jenkins, Connor Relleen

Also present: Councillors: Leonard Crosbie (Chairman of Scrutiny & Overview Committee), Paul Clarke

Officer: Katharine Eberhart, Director of Corporate Resources

1. ELECTION OF CHAIRMAN

Councillor Brian O'Connell was elected as Chairman of the Working Group for the ensuing year. It was also agreed by the Working Group that John Chidlow would be Vice-Chairman for the ensuing year.

2. TIME OF MEETINGS

The meetings of the Business Improvement Working Group would be held at 6.00pm for the ensuing year.

3. TO APPROVE AS CORRECT THE RECORD OF THE MEETING HELD ON 4TH MARCH 2015

The notes of the meeting held on 4th March 2015 were approved as a correct record. The Chairman went through the minutes in some detail for the benefit of new members of the Working Group.

4. DECLARATIONS OF INTEREST

There were no declarations of interest.

5. ANNOUNCEMENTS FROM THE CHAIRMAN OR CHIEF EXECUTIVE

There were no announcements.

6. TO APPROVE THE WORKING GROUP'S TERMS OF REFERENCE

The Terms of Reference were approved by the Working Group. It was noted that these terms would be scoped for any large scale projects that were undertaken.

4. REVIEW OF WORK PROGRAMME FOR 2015/16

Development Management Performance

The Chairman advised that the performance of the Development Management team had improved significantly as a result of the new structure and changes introduced by the Director of Planning, Economic Development & Property. It was therefore confirmed that the Working Group did not need to continue to monitor its performance.

Property and asset management

The restructure of this department had been approved in March and was now being implemented. The Property and Facilities Manager would provide an update at the next Working Group meeting in October.

Business Transformation Programme

The Chairman advised that the Working Group would not be required to review the office move to Parkside. The Business Transformation Advisory Group, of which the Chairman was a member, would be assessing the outcomes of the move and the Chairman would feed back the conclusions of the Advisory Group to the Working Group.

Financial Impact of the Overturn of Decisions on Appeal

Now that the Horsham District Planning Framework (HDPF) was nearly finalised, the issue of the overturn of appeals owing to the lack of a five year land supply for housing would no longer be relevant. Therefore the issue would not require further discussion by the Working Group.

However it was agreed that statistics regarding appeals should continue to be monitored, and those gathered prior to the adoption of the HDPF should be compared to future statistics after its adoption later this year.

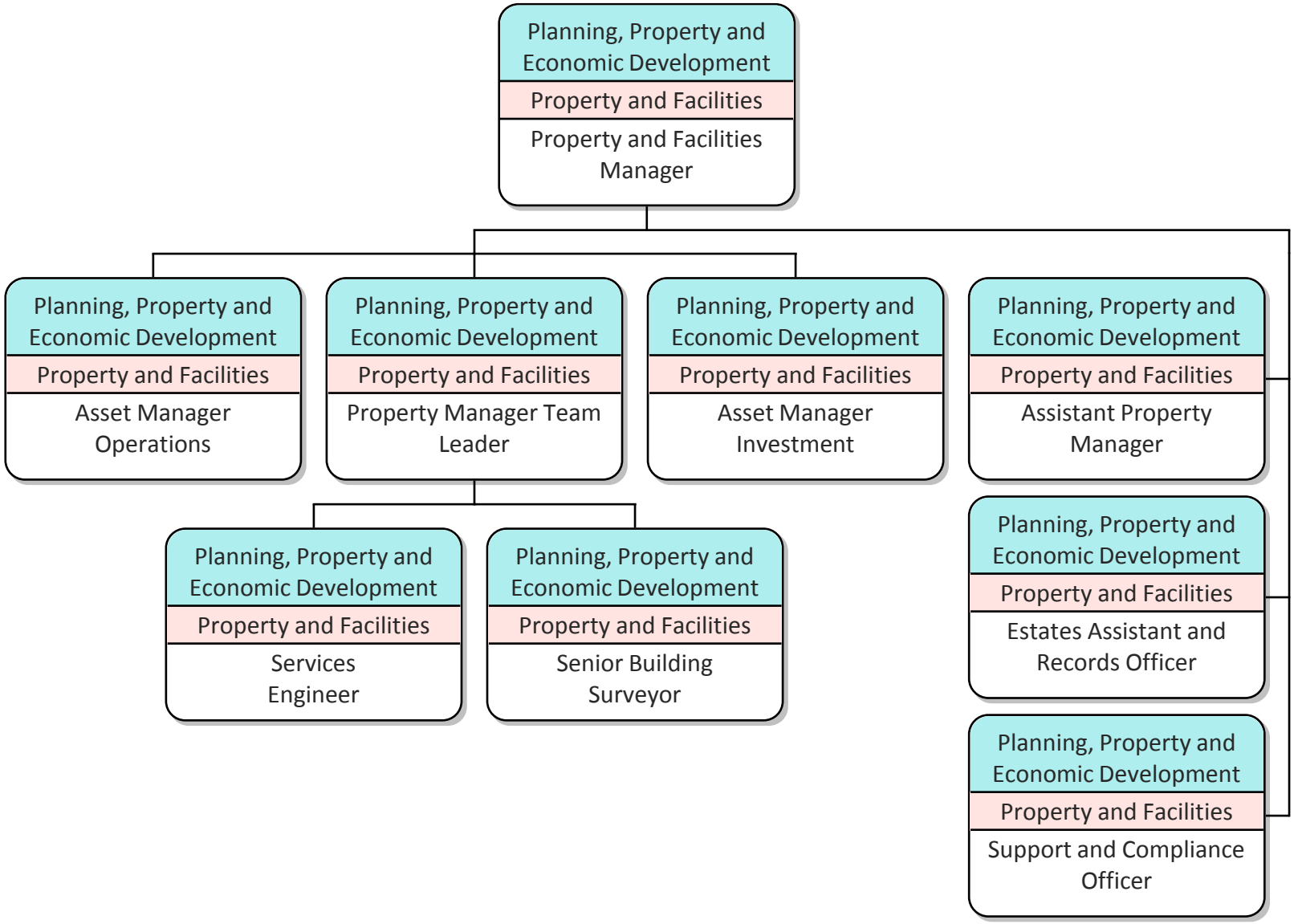
The Chairman of Scrutiny & Overview Committee advised that the Finance & Performance Working Group had questioned why one planning appeal had been taken to the High Court, resulting in substantial costs. The Chief Executive would provide a briefing to Members explaining the appeal process and when a case would be referred to the High Court.

It was confirmed that the Scrutiny & Overview Committee would be agreeing its Working Programme at its next meeting on 14th September 2015.

The meeting finished at 6.15pm having commenced at 5.30pm

CHAIRMAN

Property and Facilities Department



Report to Business Improvement Working Group

13th October 2015

By the Senior Responsible Officer, Head of Legal and Democratic Services

For Noting

Not exempt

Annual Member Overview of Horsham District Council's Corporate Policy & Procedures Document on the Regulation of Investigatory Powers Act 2000

Executive Summary

The purpose of this report is to give Members an opportunity to ensure that Horsham District Council's Corporate Policy & Procedures Document for The Regulation of Investigatory Powers Act 2000 ("The Policy") is fit for purpose. The Policy has been reviewed and amended to reflect the changes made by the Regulation of Investigatory Powers (Directed Surveillance and Covert Human Intelligence Sources) Order 2010, the Revised Code of Practice pursuant to section 71 of the Regulation of Investigatory Powers Act 2000, the Protections of Freedom Act 2012 and the Regulation of Investigatory Powers (Directed Surveillance and Covert Human Intelligence Sources) (Amendment) Order 2012. It is good practice for the Council's Policy and use of RIPA powers to be brought before Members annually. The Policy and use of RIPA powers were last considered by the Business Improvement Working Group on 8th July 2014.

Recommendations

The Business Improvement Working Group is recommended:

i) To note that the Policy remains fit for purpose and;
ii) To note that the Council has not needed to use the powers contained within RIPA during the municipal year 2014/15 and to the date of this report.

Reasons for Recommendations

To comply with Home Office RIPA Covert Surveillance and Property Interference Revised Code of Practice pursuant to section 71 of the Regulation of Investigatory Powers Act 2000, the Regulation of Investigatory Powers (Directed Surveillance and Covert Human Intelligence Sources) Order 2010, the Regulation of Investigatory Powers (Directed Surveillance and Covert Human Intelligence Sources) (Amendment) Order 2012, the Regulation of Investigatory Powers Act 2000 ("RIPA") and the Protection of Freedoms Act 2012. In particular, paragraph 3.30 of the Revised Code of Practice states that: elected members of a local authority should review the authority's use of the 2000 Act and set the policy at least once a year. The Policy is appended to this report (appendix 1).

Background Papers

i) Report to Scrutiny and Overview Committee 10 May 2010
ii) Office of Surveillance Commissioners Inspection Report June 2011
iii) Report to Business Improvement Working Group 23 October 2012
iv) Report to Business Improvement Working Group 23 April 2013
v) Report to Full Council 26 June 2013
vi) Report to Business Improvement Working Group 8 July 2014

Wards affected: All

Contact Paul Cummins **Extn**: 5435

Background Information

1. Introduction

The purpose of this report

1.1 The main purpose of this report is to provide Members with an update as to the Council's use of the Policy. Members are further asked to note that the Policy remains fit for purpose and complies with the Home Office RIPA Covert Surveillance and Property Interference Revised Code of Practice, the Regulation of Investigatory Powers (Directed Surveillance and Covert Human Intelligence Sources) Order 2010, the Regulation of Investigatory Powers (Directed Surveillance and Covert Human Intelligence Sources) (Amendment) Order 2012, the Regulation of Investigatory Powers Act 2000 ("RIPA") and the Protection of Freedoms Act 2012.

Background/Actions taken to date

1.2 The Office of Surveillance Commissioners (the "OSC") inspected the Council on 21 October 2005, following which the Council prepared and implemented its RIPA policy to reflect the outcome and feedback from the inspection.

1.3 On 12 October 2006 the Council's Cabinet:

1.3.1 Approved the Corporate Policy and Procedure Document on the Regulation of Investigatory Powers Act 2000; and
1.3.2 Authorised the Council Secretary and Solicitor to update, amend, delete add/or substitute relevant provisions as necessary.

1.4 The OSC carried out a further inspection on 05 June 2008 and as a result of feedback from this inspection, a number of amendments and additions were made to the Council's policy. The Policy was then further amended in September 2010 to reflect the changes brought about by the 2010 Order and the new Code of Conduct.

1.5 The OSC then inspected the Council on 16 June 2011. Whilst the Inspector reviewed the Council's Policy, there were no recommendations to amend the policy in any way.

1.6 On 10 July 2012, the Business Improvement Working Group recommended that the Council revise part of its Corporate Policy to reflect the legislative changes to RIPA, the Protection of Freedoms Act 2012 and the Regulation of Investigatory Powers (Directed Surveillance and Covert Human Intelligence Sources) (Amendment) Order 2012.

1.7 The Corporate Policy was revised to reflect all changes to RIPA and was subsequently adopted by Full Council on 26 June 2013. The Policy now includes the requirement to obtain:

1.7.1 Internal authorisation by the Authorised Officers before the Council uses a RIPA technique; and
1.7.2 Judicial Approval to bring its RIPA authorisation into effect.

The OSC inspected the Council on 20 May 2014, which resulted in minor amendments being suggested to the Council's RIPA Policy in response to recommendations in the OSC report, and to reflect changes in management restructure. The Policy has recently been reviewed by the Head of Legal and Democratic Services.

2. Statutory and Policy Background

Statutory background

2.1 The Regulation of Investigatory Powers Act 2000 (RIPA).

2.2 The Regulation of Investigatory Powers (Directed Surveillance & Covert Human Intelligence Sources) Order 2010.

2.3 Home Office RIPA Covert Surveillance and Property Interference Revised Code of Practice pursuant to section 71 of RIPA.

2.4 The Protection of Freedoms Act 2012.

2.5 The Regulation of Investigatory Powers (Directed Surveillance and Covert Human Intelligence Sources) (Amendment) Order 2012.

Relevant Council policy

2.6 Horsham District Council's Corporate Policy & Procedures Document on RIPA.

3. Details

The Code of Practice Requirements

3.1 Paragraph 3.30 of the Revised Code of Practice states that:

Elected members of a local authority should review the authority's use of the 2000 Act and set the policy at least once a year. They should also consider internal reports on use of the 2000 Act on at least a quarterly basis to ensure that it is being used consistently with the local authority's policy and that the policy remains fit for purpose. They should not, however, be involved in making decisions on specific authorisations.

The Policy

3.3 The Policy is based on the requirements of RIPA. It has been amended in response to inspections by the OSC, legislative and Code of Practice amendments and Management Restructure of the Council.

3.4 A copy of the Council's Corporate Policy 2015 is attached as Appendix 2.

It should be noted that the Council has not used the powers contained within RIPA during the municipal year 2014/15 and to the date of this report.

4. Next Steps

4.1 The policy will next be reviewed in accordance with paragraph 3.30 of the Revised Code of Practice and will be presented to Members by 31 December 2016.

5. Outcome of Consultations

5.1 The Head of Legal and Democratic Services has confirmed that the Policy complies with RIPA and the Revised Code of Practice.

6. Other Courses of Action Considered but Rejected

6.1 The Scrutiny & Overview Committee on 05 May 2010 agreed that this report would go to the Business Improvement Working Group and the Chairman agreed.

7. Staffing Consequences

7.1 There are no staffing consequences associated with this report.

8. Financial Consequences

8.1 There are no direct financial consequences as a result of this report.

Appendix 1

Consequences of the Proposed Action

What are the risks associated with the proposal? Risk Assessment attached Yes/No	Failure to follow the Code of Practice and RIPA legislation and for Members to review the Policy may result in the Council being criticised by the Office of Surveillance Commissioners. Failure to comply with the correct authorisation process might result in a Justice of Peace refusing to approve the grant or renewal of a RIPA authorisation or notice or refusing to approve the grant or renewal and quash the authorisation or notice. No
How will the proposal help to reduce Crime and Disorder?	Section 17 of the Crime and Disorder Act 1998 requires the Council to do all that it reasonably can to reduce crime and disorder. It is imperative that those officers whose duties may require them to investigate crimes and to use covert surveillance are aware of the duties and requirements of RIPA. Failure to comply with RIPA obligations may result in evidence being inadmissible and this may harm any prosecution or enforcement action.
How will the proposal help to promote Human Rights?	Article 8 of the Human Rights Act 1998 requires the District Council, and organisations working on its behalf, to respect the private and family life of citizens, their home and their correspondence. This is a qualified right. The District Council may interfere in the citizen's right if it is in accordance with the law. RIPA provides a statutory mechanism (within the law) for authorising covert surveillance and the use of undercover agents. RIPA ensures that any interference with Article 8 rights is necessary and proportionate.
What is the impact of the proposal on Equality and Diversity? Equalities Impact Assessment attached Yes/No/Not relevant	Having robust and regularly monitored policies in force will aid the Council in complying with equality and diversity legislation. No
How will the proposal help to promote Sustainability?	This report will not have an impact on Sustainability.

HORSHAM DISTRICT COUNCIL

Corporate Policy & Procedures Document

On

The Regulation of Investigatory Powers Act 2000

(RIPA)

~~Sue McMillan~~Paul Cummins
Senior Responsible Officer
Head of ~~Financial and~~ Legal and Democratic Services
Telephone: 01403 ~~215302~~215435
Email: ~~sue.mcmillan@horsham.gov.uk~~paul.cummins@horsham.gov.uk

Version 1: July 2006
Version 2: July 2008
Version 3: September 2010
Version 4: September 2012
Version 5: March 2013
Version 6: September 2014
Version 7: September 2015

CONTENTS

A. Corporate Policy Statement

1. The Council takes seriously its statutory responsibilities and will, at all times, act in accordance with the law and take necessary and proportionate action when undertaking surveillance as permitted under the Regulation of Investigatory Powers Act 2000 ("RIPA") and related legislation. For this purpose, the Head of Financial and Legal Services is duly authorised to keep this document up to date and amend, delete, add or substitute relevant provisions, as necessary.

2. It is this Council's Policy that:

   2.1 All covert surveillance exercises for the purposes of preventing or detecting crime or of preventing disorder conducted by the Council comply with the requirements of the Regulation of Investigatory Powers Act 2000 and related legislation;
   2.2 Only the Authorised Officers for the Department proposing to undertake covert surveillance are permitted to authorise a covert surveillance operation;
   2.3 No Authorised Officer should authorise a covert surveillance operation until he or she has demonstrated that he or she has the competence to do so;
   2.4 The Council shall only grant an authorisation for the use of Directed Surveillance where the Council is investigating particular offences, in particular, those which meet the crime threshold;
   2.5 The Council shall carry out a covert technique following an order granted by a Justice of Peace that approves the internal authorisation;
   2.6 A Covert Human Intelligence Source shall only be used rarely and in exceptional circumstances; and
   2.7 The Council shall consider the guidance provided by the Home Office and ensure that it adheres to the RIPA provisions effectively.

3. The Council's Constitution and in particular the provisions of the Scheme of Delegation to Officers as set out in Part 3F empowers the following officers to grant, review, renew and cancel authorisations under the Regulation of Investigatory Powers Act 2000:

   3.1 Tom Crowley, Chief Executive;
   3.2 Natalie Brahma-Pearl, Director of Community Services;
   3.3 Katharine Eberhart, Director of Corporate Resources;
   3.4 Chris Lyons, Director of Planning, Economic Development and Property.
   ~~Head of Housing and Community Development;~~
   ~~3.5 Head of Leisure and Economic Development;~~
   ~~3.6 Head of Financial and Legal Services;~~
   ~~3.7 Head of Corporate Support Services;~~
   ~~3.8 Head of Planning and Environmental Services, and~~
   ~~3.9 Head of Operational Services.~~

4. Following an Office of Surveillance Commissioners ("OSC") inspection on 21 October 2005 this document was prepared to reflect the outcome of and feedback from the inspection.

5. On 12 October 2005 the Council's Cabinet:

   5.1 approved the Corporate Policy and Procedure Document on RIPA and;
   5.2 authorised the Council Solicitor to update, amend, delete add or substitute relevant provisions as necessary.

6. Following an OSC inspection on 05 June 2008 this document was amended to reflect feedback from the inspection. Further amendments were made in September 2010 as a result of legislative changes.

7. Significant amendments were made to this document in Autumn 2012 to reflect legislative changes under Chapter II of Part 2 of the Protection of Freedoms Act 2012 ("PFA") which amends RIPA and requires the Council to obtain judicial approval before using covert investigatory techniques. The changes will require the Council to:

   7.1 Obtain internal authorisation by the Authorised Officers before it uses a RIPA technique; and
   7.2 Obtain Judicial Approval to bring its RIPA authorisation into effect (an order approving the authorisation or notice is granted by a Justice of the Peace (JP).

B. Definitions

RIPA	The Regulation of Investigatory Powers Act 2000
Authorised Officers	RIPA refers to "Designated Officers". For ease of understanding and application this document refers to Authorised Officers. These Authorised Officers are referred to in Appendix 1 and may include other officers who are duly added to or substituted by the Senior Responsible Officer. The Authorised Officer's responsibilities are set out in section C of this document.
Senior Responsible Officer	is the Head of ~~Financial and~~ Legal and Democratic Services. The Senior Responsible Officer's responsibilities are set out in section C of this document.
Central Register	The Central Register will contain copies of RIPA authorisations, cancellations, renewals and Magistrates Orders (where appropriate) and shall be retained by the Senior Responsible Officer.
Members	Elected Members of Horsham District Council. Members' responsibilities are set out in Section C of this document.
SPOC	The Home Office accredited "Single Point of Contact". The SPOC's responsibilities are set out in section H of this document.
CHIS	A "Covert Human Intelligence Source". Details about the role, conduct and use of a CHIS are set out in section G of this document.
PFA	The Protection of Freedoms Act 2012.
Office of Surveillance Commissioners ("OSC")	The Office of Surveillance Commissioners is the statutory body to monitor compliance with RIPA. The Council is regularly inspected by the OSC. .

C. Introduction

This Corporate Policy and Procedures document is based on the requirements of the Regulation of Investigatory Powers Act 2000 ("RIPA"), related legislation and guidance, including but not limited to:

(i) The Home Office's Code of Practice for Directed Surveillance Covert Human Intelligence Sources ("CHIS") and Disclosure of Communications Data;
(ii) The Regulation of Investigatory Powers (Communications Data) Order 2003;
(iii) The Regulation of Investigatory Powers (Directed Surveillance and Covert Human Intelligence Sources) Order 2010;
(iv) The Protections of Freedoms Act 2012;
(v) The Regulation of Investigatory Powers (Directed Surveillance and Covert Human Intelligence Sources) (Amendment) Order 2012 (SI 2012/1500)
(vi) The non-statutory Home Office's Guidance to Local Authorities in England and Wales on the judicial approval process for RIPA and the crime threshold for Directed Surveillance; and
(vii) The non-statutory Home Office's Guidance for Magistrates' Courts in England and Wales for a Local Authority application seeking an order approving the grant or renewal of a RIPA authorisation or notice.

RIPA regulates the use of investigatory powers exercised by various bodies, including local authorities, and ensures that these powers are used in accordance with the human rights of individuals who are subject to surveillance.

The investigatory powers which are relevant to a local authority are directed covert surveillance for specific operations or specific investigations and the use of Covert Human Intelligence Sources. RIPA specifies when certain types of surveillance are permitted, the extent of the surveillance and specifies who can authorise the use of RIPA.

The authoritative position on RIPA is the Act itself and any officer who is unsure about any aspect of this Corporate Policy and Procedures document should contact the Senior Responsible Officer for advice and assistance. All Authorised Officers, other Senior Managers and operational officers who have received appropriate training may apply for an authorisation. Refresher training will be organised as and when appropriate.

Copies of this document are available on the internet and intranet. The relevant forms are also available on the intranet.

Individuals with responsibilities in promoting compliance with this Corporate Policy and Procedures document are the Senior Responsible Officer, Authorised Officers and Members.

Responsibilities of the Senior Responsible Officer, Authorised Officers, and Members)

Senior Responsible Officer

1. The Senior Responsible Officer is the Head of ~~Financial and~~ Legal and Democratic Services. The Senior Responsible Officer is responsible for:

    1.1. The integrity of the process in place to authorise surveillance and interference with wireless telegraphy;
    1.2. compliance with the Act;
    1.3. engagement with the OSC and inspectors when they conduct their inspections;
    1.4. where necessary, overseeing the implementation of any post-inspection action plans recommended or approved by an OSC officer; and
    1.5. Maintaining and checking the Central Register of all authorisations, reviews, renewals, cancellations and rejections. Following the completion of internal procedures, any judicial approval, reviews, renewals, or rejections should also be retained within the Central Register.

2. The Senior Responsible Officer will ensure that all Authorised Officers and Members are made fully aware of and receive copies of this document.

Authorised Officers

3. It will be the responsibility of Authorised Officers to ensure that relevant members of staff are also suitably trained as Applicants (staff who will complete the relevant forms for a RIPA authorisation and approval) so as to avoid common mistakes appearing on Authorisation forms.

4. Authorised Officers must ensure that staff who report to them follow this document and do not undertake any form of surveillance without first obtaining the relevant internal authorisation and where appropriate judicial approval in compliance with this document.

5. Authorised Officers must pay particular attention to Health and Safety concerns and issues that may be raised by any proposed surveillance activity. Under no circumstances should an Authorised Officer authorise any RIPA form unless and until they are satisfied that the health and safety of the employee or agent are properly considered, addressed, the risks of which are minimised, and the activity is necessary and proportionate to the surveillance being proposed.

6. It is the responsibility of the relevant Authorised Officers to ensure that the Senior Responsible Officer receives the relevant completed form within one week of completion.

7. Authorised Officers must ensure that when sending copies of any forms to the Senior Responsible Officer for inclusion in the Central Register, that they are sent in **sealed** envelopes and marked "**Strictly Private & Confidential - RIPA"**.

8. Authorised Officers must ensure that requests for access to and disclosure of Communications Data under RIPA and the Regulation of Investigatory Powers (Communication Data) Order 2003, are made through the Council's accredited SPOC.

Members

9. Members will monitor the Council's use of RIPA and consider this Corporate Policy & Procedures Document at least annually and refer to Council if there are any concerns. Members will consider internal reports on the Council's use of the RIPA on a quarterly basis to ensure that staff are complying with this Corporate Policy and Procedures Document in a consistent manner, and that it remains fit for purpose.

10. The Senior Responsible Officer will prepare a quarterly report which will state the number of internal authorisations and judicial approvals in the previous quarter and a brief outline of the reasons for the Council's use of RIPA.

Review of Council's RIPA Corporate Policy and Procedures Document

11. RIPA and this document are important to the effective and efficient operation of the Council's action with regard to the use of covert surveillance and Covert Human Intelligence Sources. This document will be kept under review by Members & the Senior Responsible Officer. Authorised Officers must bring suggestions for continuous improvements to the attention of the Senior Responsible Officer at the earliest opportunity.

Risks of non-compliance with this Corporate Policy and Procedure Document

12. RIPA provides a legal framework for a public authority to authorise conduct which engages Article 8 ECHR. It does this by ensuring that use of the relevant techniques are authorised only if the tests of necessity, proportionality and legitimate aim are satisfied.

13. Where there is an interference with the right to respect for private life and family life that may engage Article 8 of the European Convention on Human Rights 1950, and where there is no other source of lawful authority for the interference or if the use of RIPA is held not to be necessary or proportionate to the circumstances, the consequences of not obtaining or following the correct authorisation procedure may be that the action and the evidence obtained, is held to be inadmissible by the Courts pursuant to Article 6 European Convention on Human Rights 1950.

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

15. Requests for authorisation under RIPA must be considered by designated senior officers and detailed records must be kept by the Council. As the Surveillance Commissioner, the Interception of Communications Commissioner and the Investigatory Powers Tribunal can oversee the Council's use of RIPA, it is essential that the Council follows this Corporate Policy and Procedures document.

16. If the correct procedures are not followed, a complaint of maladministration could be made to the Local Government Ombudsman, and/or the Council could be ordered to pay compensation. Such action would not, of course, promote the Council's reputation and will, undoubtedly, be the subject of adverse press and media interest.

17. The Council's use of RIPA may be considered by the Office of Surveillance Commissioner's and the Investigatory Powers Tribunal. Further details are set out in section J.

18. It is essential, therefore, that all involved with RIPA comply with this document and any further guidance that may be issued, from time to time, by the Senior Responsible Officer. A flow chart of the internal procedures to be followed is set out within Appendix 2.

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

D. RIPA

1. The Council, as a public authority, is not to act in a way that is incompatible with the rights protected under the European Convention for the Protection of Human Rights and Fundamental Freedoms 1950 (the "ECHR"). The Human Rights Act 1998 (which brought much of the ECHR into domestic law) requires the Council, and organisations working on its behalf, to also meet this obligation.

2 The investigatory powers which are relevant to the Council and require consideration of human rights are:

   2.1 Directed covert surveillance for specific operations or specific investigations;
   2.2 The use of Covert Human Intelligence Sources; and
   2.3 Obtaining and disclosing Communications Data.

3. RIPA does not allow the use of any other covert techniques by the Council to be authorised. In particular, the Council cannot be authorised under RIPA to intercept the **content** of a communication.

In accordance with the law

4. RIPA provides a statutory mechanism (meeting the test of "in accordance with the law") for authorising Directed Covert Surveillance, the use of Covert Human Intelligence Sources (a "CHIS") e.g. undercover agents and obtaining and disclosing Communications Data. RIPA 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, the RIPA seeks to ensure that both the public interest and the human rights of individuals subject to surveillance are suitably balanced.

5. In accordance with Article 8 ECHR the Council and organisations working on its behalf must respect the private and family life of citizens, their home and their correspondence. This is, however, a qualified right, as the Council may interfere in the citizen's right if it is in accordance with the law, is necessary in a democratic society and is proportionate.

6. Accordingly, in certain circumstances, the Council may interfere with the Article 8 rights, if such interference is:

   6.1 in accordance with the law;
   6.2 necessary; and
   6.3 proportionate.

7. A RIPA authorisation may only be granted if the Authorised Officer believes that the conduct is necessary and proportionate for one or more of the statutory purposes. The Regulation of Investigatory Powers (Directed Surveillance and Covert Human Intelligence Sources) Order 2010 and the Regulation of Investigatory Powers (Communications Data)

Order 2010 provide that the Council may only authorise the use of covert techniques for the purpose of "the prevention or detection of crime or the prevention of disorder".

8. 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.

Necessary and proportionate

9. When the Council seeks to use its powers under RIPA, and has determined that its actions would be in accordance with the law, it must consider whether the surveillance or use of the CHIS is **necessary** to the particular operation or enquiry and whether the surveillance or sourcing suggested is **proportionate**:

    9.1 Firstly, RIPA requires that the person granting an authorisation believes that the authorisation is necessary in the circumstances of a particular case e.g. one or more of the statutory grounds in section 28(3) RIPA for directed surveillance applies;

    9.2 Secondly, if the activities are necessary, the person granting the authorisation must believe that the activities are proportionate to what is sought to be achieved by carrying them out. The following factors should be considered as set out in paragraph 3.6 of the Home Office Code of Practice:

        9.2.1 Balancing how intrusive the activity is on the individual and/or others who might be affected by the surveillance against the need for the surveillance activity:

        9.2.2 Balancing the size and scope of the proposed activity against the gravity and extent of the perceived crime or offence;

        9.2.3 Explaining how and why the methods to be adopted will cause the least possible intrusion on the subject and others;

        9.2.4 Considering whether the activity is an appropriate use of the legislation and a reasonable way, having considered all reasonable alternatives, of obtaining the necessary result;

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

    9.3 The surveillance activity will not be proportionate if it is excessive in the circumstances of the case or if the information which is sought could reasonably be obtained by other less intrusive means. All such activity should be carefully managed to meet the

objectives of the surveillance in question and must not be arbitrary or unfair;

9.4 Lastly, Authorised Officers must consider the risk of "collateral intrusion", which is intrusion on, or interference with, the privacy of persons other than the individual subject of surveillance. Measures must be taken wherever practicable to avoid unnecessary collateral intrusion and minimise any intrusion of individuals not directly connected with the investigation or operation.

10. Directly employed Council staff and external agencies working for the Council may be permitted to assist the Council when using RIPA powers for the time they are working for or on behalf of the Council. All external agencies must, therefore, comply with RIPA and any legislation relating to Data Protection and Equalities.

11. Any activity 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 officers identified in Appendix 1 and may include other officers who are duly added to or substituted by the Senior Responsible Officer.

12. RIPA does:

12.1 require prior authorisation and judicial approval of directed surveillance;
12.2 prohibit the Council from carrying out intrusive surveillance;
12.3 require authorisation of the conduct and use of a CHIS; and
12.4 require safeguards for the conduct and use of a CHIS.

13. RIPA does not:

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

If the Authorising Officer or any Applicant is in any doubt, they should ask the RIPA Co-ordinating Officer BEFORE any directed surveillance and/or CHIS is authorised, renewed, cancelled or rejected.

RIPA and use of email

14. In terms of monitoring e-mails and internet usage, it is important to recognise the interplay and overlap with the Council's e-mail and internet policies and guidance, the Telecommunications (Lawful Business Practice)(Interception of Communications) Regulations 2000, the Data Protection Act 1998 and its related guidance and Codes of Practice.

RIPA forms should only be used where **relevant** and they will only be **relevant** where the **criteria** listed on the forms is fully met.

15. Logs of access to the Internet and use of e-mail are maintained by the Head of ~~Corporate Support Services~~CenSus ICT. With effect from 05 January 2004 local authorities gained new powers and responsibilities under RIPA to access Communications Data (for the purpose of preventing or detection of crime or preventing disorder) by virtue of the Regulation of Investigatory Powers (Communications Data) Order 2003 ("the 2003 Order") which brought into effect the provisions of Chapter II of RIPA. Requests for access to and disclosure of such data will only be able to be made through a Designated Officer (in accordance with RIPA and the 2003 Order) who is also a Home Office accredited Single Point of Contact ("SPOC"). The Council will continue to ensure that it has at least one accredited SPOC in place for this purpose.

E. Types of Surveillance and Definitions

1. 'Surveillance' is defined at section 48(2) RIPA and includes:

1.1 monitoring, observing or listening to persons, their movements, their conversations or their other activities or communications;
1.2 recording anything monitored, observed or listened to in the course of surveillance;
1.3 surveillance by or with the assistance of a surveillance device (any apparatus designed or adapted for use in surveillance).

Surveillance can be either overt or covert.

2. **Overt Surveillance**

2.1 Most surveillance carried out by the Council will be overt, as there will be nothing secretive, clandestine or hidden about the surveillance. In many cases, officers' behaviour will be the same as a member of the public (for example in the case of most test purchases), and/or will be going about Council business openly (for example a Neighbourhood Warden walking through the estate).
2.2 Surveillance will be overt if the subject of the surveillance has been informed that it will occur (for example where a noisemaker is warned (preferably in writing) that noise will be recorded if the noise continues, or where an entertainment licence is issued subject to conditions, and the licensee is told that officers may visit without notice or identifying themselves to the Owner/Proprietor to check that the conditions are being met.)

3. Covert Surveillance

3.1 Covert Surveillance is carried out in a manner designed to ensure that the person subject to the surveillance is unaware of it taking place (section 26(9)(a) of RIPA).
3.2 RIPA regulates two types of covert surveillance, (Directed Surveillance and Intrusive Surveillance) and the use of CHIS.

4. Intrusive Surveillance

4.1 Intrusive Surveillance is when the Surveillance activity:
4.1.1 Is covert;
4.1.2 Is carried out in relation to anything taking place on any residential premises (including hotel bedrooms, prison cells and rented accommodation), or in any private vehicle (including hire or company cars, boats or caravans). The Office of the Surveillance Commissioner's guidance says that gardens and driveways are not included within the definition of "residential premises"); and
4.1.3 Involves the presence of a person in the premises or in the vehicle or is carried out by a surveillance device.

4.2 Surveillance of premises used for legal consultation is also to be treated as Intrusive Surveillance e.g. any place of business of any professional legal advisor.

4.3 Surveillance equipment mounted outside the premises or vehicle will not be intrusive, unless the device consistently provides information of the same quality and detail as might be expected if they were in the premises or vehicle.

FOR THE AVOIDANCE OF DOUBT:

- Council officers must not carry out Intrusive Surveillance; and
- Intrusive Surveillance can only be carried out by the Police and other Law Enforcement Agencies.

5. **Directed Surveillance**

5.1 Directed Surveillance is defined in section 26(2) RIPA as surveillance which:

5.1.1 Is covert but not intrusive surveillance (**the Council must not carry out any intrusive surveillance**);

5.1.2 is undertaken for the purpose of a **specific investigation** or specific operation in such a manner as is **likely to** result in the **obtaining of private information** about a person (whether or not one specifically identified for purposes of an investigation or operation); and

5.1.3 Is not carried out in an immediate response to events which would otherwise make seeking authorisation under the Act unreasonable, for example, spotting something suspicious and continuing to observe it.

Likely to** result in the **obtaining Private Information

5.2 "Private information" in relation to a person includes any information relating to his private and family life, his home and his correspondence. The fact that covert surveillance occurs in a public place or on business premises 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 that person and others with whom he or she comes into contact, or is an associate.

5.3 Although overt town centre CCTV cameras do not normally require authorisation, if the camera is tasked for a specific purpose, which involves prolonged surveillance on a particular person, authorisation will be required. The way a person runs their business may also reveal information about his or her private life and the private lives of others.

6. Confidential Information

6.1 Particular care should be taken in cases where the subject of the investigation might reasonably expect a high degree of privacy where confidential information is involved.

6.2 "Confidential Information" consists of such matters as legal privilege, confidential personal information or sensitive personal data (as defined within the Data Protection Act 1998) or confidential journalistic information.

6.3 Where the Council is likely to obtain confidential information through its use of surveillance, the authorisation for such surveillance must be provided by the Chief Executive or in his absence his nominated Deputy, instead of any Authorised Officer.

6.4 "Legally Privileged information" applies to communications between a professional legal adviser and their client or any person representing their client which are made in connection with the giving of legal advice to the client or in contemplation of legal proceedings.

6.5 The Council is permitted to use its RIPA powers to obtain information including Legally Privileged information. However, such an application for obtaining Legally Privileged Information should only be made in exceptional and compelling circumstances. Particular regard should be given to the test of proportionality. Similar considerations should also be given to authorisations that involve Confidential Personal Information and Confidential Journalistic Material.

6.6 "Confidential Personal Information" is information held in confidence relating to the physical or mental health or spiritual counselling information held by Ministers of religion concerning an individual (whether living or dead) who can be identified from that information. Examples include consultation notes or correspondence between a Health Professional and a patient.

6.7 'Confidential Journalistic Material' includes material acquired or created for the purposes of journalism subject to an undertaking to hold it in confidence.

7. For the purposes of RIPA:

7.1 Surveillance is covert if, and only if, it is carried out in a manner that is calculated to ensure that persons who are subject to the surveillance are unaware that it is or may be taking place;

7.2 A purpose is covert, in relation to the establishment or maintenance of a personal or other relationship, if and only if the relationship is conducted in a manner that is calculated to ensure that one of the parties to the relationship is unaware of the purpose; and

7.3 A relationship is used covertly, and information obtained is disclosed covertly, if and only if it is used or, as the case may be, disclosed in a manner that is calculated to ensure that one of the parties to the relationship is unaware of the use or disclosure in question.

FOR THE AVOIDANCE OF DOUBT:

- Only those officers 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, he or she must NOT carry out or approve/reject any request made under this document; and
- Where relevant, Officers of the Council, its agents or persons acting on behalf of the Council must only carry out the Surveillance activity when judicial approval has been granted.

8. **Examples of different types of Surveillance**

Type of Surveillance	**Examples**
Overt Surveillance	§ Police Officer or Parks Warden on patrol. § Sign-posted Town Centre CCTV cameras (in normal use). § Recording noise coming from outside the premises after the occupier has been warned that this will occur if the noise persists. § Most test purchases (where the Officer behaves no differently from a normal member of the public).
Covert Surveillance but not requiring prior RIPA authorisation	§ CCTV cameras providing general traffic, crime or public safety information.
Directed Surveillance requiring prior RIPA authorisation	§ Officers follow an individual or individuals over a period, to establish whether he or she is in employment when claiming benefit or off long term sick from employment. § Test purchases where the officer has a hidden camera or other recording device to record information that might include information about the private life of a shop-owner, for example, where he or she is suspected of operating their business in an unlawful manner.
Intrusive Surveillance - The Council must NOT carry out this type of surveillance	§ Planting a listening or other device ("bug") in a person's home or in their private vehicle.

The statutory RIPA Code of Practice on Covert Surveillance and Property Interference sets out 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.

RIPA does not apply in circumstances where members of the public volunteer information to the Council via contact numbers set up to receive information.

NOTE: If the Council acts covertly but Article 8 rights are not engaged, then no RIPA authorisation is necessary e.g. covertly monitor traffic flows. The Council must, however, assess whether or not it requires RIPA authorisation.

F. DIRECTED SURVEILLANCE

1. Under section 28(1) RIPA, the Council may authorise the use of Directed Surveillance but will need to seek Judicial approval of the grant or authorisation under RIPA.

2. For the purposes of section 26(2) RIPA, surveillance is "directed" if it is:
   2.1 Covert, but not intrusive surveillance (i.e. it takes place somewhere other than residential premises, particular premises where legal consultations take place or private vehicles);
   2.2 Conducted for the purposes of a specific investigation or operation e.g. pre-planned against a specific individual or group;
   2.3 Likely to result in the obtaining of private information about a person (whether or not one specifically identified for the purposes of the investigation or operation); and
   2.4 Conducted otherwise than as an immediate response to events or circumstances the nature of which is such that it would not be reasonably practicable to seek an authorisation under RIPA.

3. Amendments to the Regulation of Investigatory Powers (Directed Surveillance and Covert Human Intelligence Sources) Order 2010 ("the 2010 Order") mean that the Council can now only grant an authorisation under RIPA for the use of directed surveillance where it is investigating particular types of criminal offences with a specific crime threshold.

Crime threshold

4. A RIPA authorisation may only be granted if the Authorised Officer believes that the conduct is necessary and proportionate for one or more of the statutory purposes, including but not limited to the purpose of preventing or detecting crime or of preventing disorder.

5. The appropriateness of authorising Directed Surveillance must be considered carefully as the use of Directed Surveillance is dependent on the offence under investigation. In accordance with the Regulation of Investigatory Powers (Directed Surveillance and Covert Human Intelligence Sources) Order 2010, the Council may only authorise use of directed surveillance where they are investigating meets the following conditions:

   5.1 The offence under investigation carries a custodial sentence of six months or more; or
   5.2 The offence is an offence under:
      5.2.1 Section 146 Licensing Act 2003: the sale of alcohol to children;

5.2.2 Section 147 Licensing Act 2003: allowing the sale of alcohol to children
5.2.3 Section 147A Licensing Act 2003: persistently selling alcohol to children; or
5.2.4 Section 7 of the Children and Young Persons Act 1933 the sale of tobacco etc. to persons under eighteen.

6. The Council **cannot 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.

7. It is possible that during an investigation, that the type and seriousness of offences may change. If it becomes apparent 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 Council must cease using Directed Surveillance. If a Directed Surveillance authorisation is already in force it should be cancelled via the formal channels.

8. The Council must ensure that its internal procedures are followed and authorisation is sought against a specific offence that meets the crime threshold. There will be occasions where evidence is sought and may be used for various charges, some of which may fall below the crime threshold. In these circumstances, it will be for the Courts to decide what evidence it shall admit in proceedings and the weight given to such evidence.

Authorised Officer

9. An authorisation for the carrying out of Directed Surveillance shall not be granted unless the Authorising Officer believes:

9.1 The authorisation is necessary – that the use of Directed Surveillance is necessary for the purposes of preventing or detecting crime or of preventing disorder; and
9.2 The authorised surveillance is proportionate to what is sought to be achieved by carrying out the surveillance.

What surveillance conduct is authorised?

10. The conduct that is authorised by an authorisation for the carrying out of directed surveillance is any conduct that:
10.1 consists in the carrying out of directed surveillance of any such description as is specified in the authorisation; and
10.2 is carried out in the circumstances described in the authorisation and for the purposes of the investigation or operation specified or described in the authorisation.

Confidential Information

11. Where it is likely that confidential information or matters subject to legal privilege will be sought, the Directed Surveillance may only be authorised by the Head of Paid Service, or the person acting as the Head of Paid Service.

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

1. Who is a CHIS?

1.1 Section 26(8) RIPA states that a person is a Covert Human Intelligence Source (CHIS) if:

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

(b) He or she covertly uses the relationship to obtain information or to provide access to any information to another person; or

(c) He or she covertly discloses information obtained by the use of such a relationship, or as a consequence of the existence of such a relationship.

1.2 For the purposes of this section, a relationship is used covertly, and information obtained by the use of such a relationship or as a consequence of the existence of such a relationship is disclosed covertly, **if and only if** it is used or disclosed in a manner that is calculated to ensure that one of the parties to the relationship is unaware of the use or disclosure of the information.

1.3 It is a common misperception that an informant, whether an investigator working undercover or a member of the public providing information, is not a CHIS, unless he has been tasked by the public authority to obtain information.

~~1.2~~1.4 However, there is a risk that a member of the public giving information, even if they are not tasked to do so, may in reality be a CHIS because the information that is covertly passed on to the authority has been obtained in the course of, or as a consequence of, a personal or other relationship. For example, when an informant gives repeat information about a suspect or about a family, and it becomes apparent that the informant may be obtaining that information in the course of a family or neighborhood relationship, then officers should be aware that it probably means that the informant is in reality a CHIS, to whom a duty of care is owed if the information is then used.

2. Necessity and Proportionality

2.1 Section 29(2) RIPA specifies that Authorised Officers shall not grant an authorisation for the conduct or use of a CHIS unless he or she believes:

2.1.1 that the authorisation is necessary on one of the statutory grounds, which for Council activities, would be for the prevention or detection of crime or preventing disorder;

2.1.3 that the authorised conduct or use is proportionate to what is sought to be achieved by that conduct or use; and

2.1.4 that there are arrangements for the CHIS's case in force as are necessary for ensuring that:

2.1.4.1 there will at all times be an appropriate officer (normally the Investigating Officer) who will have day-to-day responsibility for dealing with the CHIS on behalf of the Council, and for the CHIS's security and welfare;

2.1.4.2 there will at all times be another officer who will have general oversight of the use made of the CHIS;

2.1.4.3 there will at all times be an officer who will have responsibility for maintaining a record of the use made of the CHIS;

2.1.4.4 the records relating to the CHIS that are maintained by the Council will always contain particulars of all such matters as specified in the Regulation of Investigatory Powers (Source Records) Regulations 2000; and

2.1.4.5 the records maintained that disclose the identity of the CHIS will not be available to persons except to the extent that there is a need for access to them to be made available to those persons.

3. What must be authorised?

3.1 The use of a CHIS or the conduct of a CHIS requires prior authorisation:

3.1.1 **Conduct** of a CHIS is establishing or maintaining a personal or other relationship with a person for the covert purpose of (or is incidental to) obtaining and passing on information;

3.1.2 **Use** of a CHIS is the action of inducing, asking or assisting a person to act as a CHIS (including the decision to use a CHIS).

3.2 A CHIS includes undercover officers, public informants and people who make test purchases.

3.3 The Council will need to seek judicial approval of the grant or renewal of any authorisation under RIPA.

3.4 The Council is not required to provide the true identity of the CHIS either on the application form or verbally to the JP.

3.5 Additional safeguards when authorising a CHIS are required and are set out in Section I, page 32.

4. What is authorised?

4.1 The conduct that is authorised by an authorisation for the conduct or the use of a CHIS is any conduct that:

(a) is comprised in any such activities involving conduct of a CHIS, or the use of a CHIS, as are specified or described in the authorisation;
(b) consists in conduct by or in relation to the person who is so specified or described as the person to whose actions as a CHIS the authorisation relates; and
(c) is carried out for the purposes of, or in connection with, the investigation or operation so specified or described.

The Council is permitted to use a CHIS IF, AND ONLY IF, RIPA procedures detailed in this document are followed.

Security and Welfare

4.2 Before authorising the use or conduct of a source, the Authorised Officer should ensure that a risk assessment is carried out to determine:

4.2.1 The risk to the CHIS; and
4.2.2 The likely consequences if the role of the CHIS becomes known to the individual subject of the surveillance or those involved in the surveillance activity.

4.3 The Council should also consider the ongoing security and welfare of the CHIS, after the end or cancellation of the RIPA authorisation.

5. Juvenile Sources

5.1 Authorisations for juvenile sources can only be granted by the Chief Executive or in his absence his authorised Deputy. Additional safeguards must be in place where a Juvenile Source is used.

5.2 The Council cannot authorise the use of a CHIS under the age of 18 without carrying out a special risk assessment in relation to any risk of physical injury or psychological distress to the source that may arise. The Authorising Officer must also be satisfied that any risks identified are justified and have been explained to and are understood by the CHIS. If the local authority is authorising the use of a CHIS against his parents or carers particular consideration must be given to whether this is justified.

5.3 Special safeguards apply to the use or conduct of juvenile sources (i.e. under 18 year olds). On no occasion can a child under 16 years of age be authorised to give information against his or her Parents.

5.4 Where a CHIS is under the age of 16 arrangements must also include ensuring that an appropriate adult (usually a parent or carer) is present at every meeting with the Council.

6. Vulnerable Individuals

6.1 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.

6.2 A Vulnerable Individual may only act as a source in the most exceptional of circumstances.

6.3 Authorisations for the use of a Vulnerable Individual as a CHIS can only be authorised by the Chief Executive or in his absence his authorised Deputy. The authorisation to use a Vulnerable Individual as a CHIS is effective only where Judicial approval has been sought. If there is any doubt regarding sufficiency of rank of the Authorising officer, the JP shall request the Council representative obtain confirmation from the Council's Monitoring Officer.

7. Confidential Information

7.1 In cases where a CHIS is deployed and it is likely that the Council will obtain confidential information, the internal authorisation must be sought from the Chief Executive or in his absence his nominated Deputy.

7.2 "Confidential information" consists of such matters as Legal Privilege, confidential personal information or confidential journalistic information. Further details are provided in Section E above.

Matters subject to Legal Privilege

8. Where the activities of a CHIS will result in the CHIS obtaining, providing access to or disclosing matters subject to legal privilege, a local authority must obtain prior approval from the Surveillance Commissioners before authorising such conduct.

Test Purchases

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

10. Determining whether someone is a CHIS is a matter of judgment according to all the circumstances of a case. For example, 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 directed surveillance.

Anti-social Behaviour Activities (e.g. noise, violence, race etc)

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

12. Recording sound (with a DAT recorder or other similar device) on private premises could constitute intrusive surveillance, unless it is done overtly. For example, it will be possible to sound record if the noisemaker is warned that this will occur if the level of noise continues.

13. No machine should be used which pre-records or post-records without the individual being informed, as this may form Intrusive Surveillance. For example, placing a stationary or mobile video camera outside a building to record anti social behaviour on residential estates will require prior authorisation.

H. Acquisition and Disclosure of Communications Data

Communications Data

1. Under section 22(3) RIPA, the Council may authorise the acquisition of Communications Data. The Council will, however, need to seek judicial approval of the grant or renewal of an "authorisation" or of the giving or renewal of a "notice" under RIPA in accordance with sections 23A and 23B RIPA.

2. Communications Data is "who", "when", and "where" of a communication, but not the "what" – the content of what was said or written. RIPA groups Communications Data into three types:

   (i) Traffic data, which includes information about where the communications are made or received;
   (ii) Service user information, such as the type of communication, time sent and its duration; and
   (iii) Subscriber information which includes billing information such as the name, address, bank details of the subscriber of telephone or internet services.

3. Specifically, section 21(4) RIPA defines "Communications Data" to mean any of the following:

(a) any traffic data comprised in or attached to a communication (whether by the sender or otherwise) for the purposes of any postal service or telecommunications system by means of which it is being or may be transmitted;

(b) any information which includes none of the contents of a communication (apart from any information falling within paragraph (a)) and is about the use made by any person:
(i) of any postal service or telecommunications service; or
(ii) in connection with the provision to or use by any person of any telecommunications service, of any part of a telecommunication system;

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

4. Only Communications Data falling within (b) and (c) above may be authorised or required to be obtained by means of an authorisation given, or notice made on behalf of the Council under Sections 22(3) and (4) of RIPA. The Council may only acquire service user information or subscriber information.

5. "Traffic data", in relation to any communication, means:

(a) any data identifying, or purporting to identify, any person, apparatus or location to or from which the communication is or may be transmitted,
(b) any data identifying or selecting, or purporting to identify or select, apparatus through which, or by means of which, the communication is or may be transmitted,
(c) any data comprising signals for the actuation of apparatus used for the purposes of a telecommunication system for effecting (in whole or in part) the transmission of any communication, and
(d) any data identifying the data or other data as data comprised in or attached to a particular communication,

but that expression includes data identifying a computer file or computer program access to which is obtained, or which is run, by means of the communication to the extent only that the file or program is identified by reference to the apparatus in which it is stored.

Notices to a Communications Service Provider

7. Under Section 22(4) of RIPA the Council may serve a 'Notice' on a Communications Service Provider requiring them to collect or retrieve the data and produce it to the Council. The Notice is given by a Designated Person or Authorised Officer, but must be served by a SPOC.

8. Section 22(4) states that where it appears to an Authorised Officer that a postal or telecommunications operator is or may be in possession of, or be capable of obtaining, any communications data, the Authorised Officer may, by notice to the postal or telecommunications operator, require the operator:

   (a) if the operator is not already in possession of the data, to obtain the data; and
   (b) in any case, to disclose all of the data in his possession or subsequently obtained by him.

9. The authorisation or Notice under RIPA for Communications Data may only relate to Service User Information or Subscriber Information.

FOR THE AVOIDANCE OF DOUBT:

The Council can only be authorised under RIPA to obtain Communications Data where it is necessary for the purpose of preventing or detecting crime or of preventing disorder (section 22(2) RIPA).

Designated Persons or Authorised Officers

10. Designated Persons are defined within RIPA and the 2003 Order and for the purposes of this Policy are the RIPA Authorised Officers. Designated Persons or Authorised Officers may grant an authorisation via the internal authorisation procedure to permit an Officer of the Authority to collect or retrieve communications data. Such internal authorisation is not, however, effective unless and until judicial approval has been sought.

11. An authorisation under Section 22(3) of RIPA is granted by the Designated Person or Authorised Officer but must be administered by an Officer of the Council who is a Home Office accredited SPOC. The authorisation is designed to authorise an officer within the Council to engage in specific conduct.

Grounds for Authorisations and Notices

12. An Authorised Officer:
   - May only grant an authorisation or give a notice under sections 22(3) and 22(4) of RIPA where the Authorised Officer believes that obtaining Communications Data is necessary for the purpose of preventing or detecting crime or of preventing disorder; and
   - Must not grant an authorisation or give a notice, unless he believes that obtaining the data in question by the conduct authorised or required by the authorisation or notice is proportionate to what is sought to be achieved by so obtaining the data.

13. The Authorised Officer's counter signature will in all cases show the rank or title of the grade and cover a clear description in his or her own words of what is being authorised and against which subjects or location ('who,

Formatted: Font: Not Bold, No underline

what, where, when and how'). For many CD requests the forms are completed electronically, including the insertion of an electronic signature for the designated person. If there is any doubt regarding sufficiency of rank the JP should request the Council representative obtain confirmation from their Monitoring Officer who will be able to advise them.

Proportionality

14. An Authorised Officer shall not grant an authorisation unless he or she believes that obtaining the data in question by the conduct authorised or required by the authorisation or notice is proportionate to what is sought to be achieved by so obtaining the data.

15. There is no requirement to provide information about the Council's application to access Communications Data to:

15.1 Any person to whom the authorisation or notice which is the subject of the application relates; or
15.2 Any such person's legal representatives.

Form and Duration of Authorisations and Notices

16. An authorisation under section 22(3) of RIPA:
(a) must be granted in writing or (if not in writing) in a manner that produces a record of its having been granted;
(b) must describe the conduct to which the acquisition and disclosure of Communications Data (Chapter II of RIPA) applies that is authorised and the communications data in relation to which it is authorised;
(c) must specify the grounds falling within section 22(2) of RIPA by reference to which it is granted. In these circumstances, the ground should be for the purposes of purpose of preventing or detecting crime or of preventing disorder; and
(d) must specify the office, rank or position held by the person granting the authorisation.

17. A Notice under section 22(4) of RIPA requiring communications data to be disclosed or to be obtained and disclosed:
(a) must be given in writing or (if not in writing) must be given in a manner that produces a record of its having been given;
(b) must describe the communications data to be obtained or disclosed under the notice;
(c) must specify the ground falling within section 22(2) of RIPA by reference to which the notice is given. In these circumstances, the ground should be for the purposes of purpose of preventing or detecting crime or of preventing disorder;
(d) must specify the office, rank or position held by the person giving it; and
(e) must specify the manner in which any disclosure required by the Notice is to be made.

18. A notice must not require the disclosure of communications data to any person other than:
(a) the person giving the notice; or
(b) such other person as may be specified in or otherwise identified by, or in accordance with, the provisions of the notice;

but the provisions of the notice shall not specify or otherwise identify a person for the purposes of paragraph (b) unless he holds an office, rank or position with the same relevant public authority as the person giving the Notice.

19. An authorisation or notice:
(a) must not authorise or require any data to be obtained after the end of the period of one month beginning with the date on which the authorisation is granted or the notice given; and
(b) in the case of a notice, must not authorise or require any disclosure after the end of that period of any data not in the possession of, or obtained by, the postal or telecommunications operator at a time during that period.

20. An authorisation under section 22(3) RIPA or Notice under section 22(4) RIPA may be renewed at any time before the end of the period of one month applying to that authorisation or notice.

21. A renewal of an authorisation or of a notice must be by the grant or giving of a further authorisation or notice.

22. Paragraph 19 will have effect in relation to a renewed authorisation or renewal notice as if the period of one month mentioned in that paragraph did not begin until the end of the period of one month applicable to the authorisation or notice that is current at the time of the renewal.

23. Where an Authorised Officer who has given a Notice under section 22(4) is satisfied:
(a) that it is no longer necessary on the relevant grounds falling within section 22(2) of RIPA for the requirements of the notice to be complied with, or
(b) that the conduct required by the notice is no longer proportionate to what is sought to be achieved by obtaining communications data to which the notice relates,

he or she must cancel the notice.

24. Appendix 5 contains the relevant Communications Data Forms.

I. Authorisation Procedures

The process

Authorisations for the use of techniques under RIPA are granted:

1. Internally by an Authorised Officer; and
2. Approved by a Justice of the Peace at the Magistrates' Court, as RIPA authorisations are now subject of an external approval mechanism.

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 process from application consideration to the recording of information. It is the responsibility of the relevant Authorised Officer to ensure that the Senior Responsible Officer receives the relevant forms within one week of its completion.

1. Authorised Officers

Forms must only be signed by Authorised Officers who are specified within the Council's Constitution, and are listed in **Appendix 1**.

If a Director or Head of Service wishes to add, delete or substitute a post, he or she must refer such a request to the Senior Responsible Officer.

A higher level of authority is required where:

1. The Directed Surveillance or the use or proposed conduct of a CHIS is likely to produce 'confidential information'; or
2. The proposed source of a CHIS is a juvenile or the proposed conduct is by a juvenile source; or
3. The proposed source of a CHIS is a Vulnerable Individual or the proposed conduct is by a Vulnerable Individual.

In such cases the Authorisation can only be given by the Chief Executive or in his absence his Authorised Deputy.

Authorisations under RIPA are separate from Delegated Authority to act under the Council's Scheme of Delegation. RIPA authorisations are for **specific** investigations only, and must be renewed or cancelled once the specific surveillance is complete or due to expire.

Officers must ensure that the application process set out within this document is followed, so as to avoid errors which could result in a JP's refusal to grant or renew a RIPA authorisation.

2. Training Records

Training will be provided to all Authorised Officers before they are permitted to sign any RIPA Forms. Refresher training will also be provided as and when required. Authorised Officers must ensure that this training is cascaded to officers within their service teams.

Authorised Officers will be suitably trained and they must exercise their minds every time they are asked to sign a Form. They must not sign or rubber stamp Forms without thinking about their personal or the Council's responsibilities.

3. Application Forms

Only the RIPA forms set out in this Document must be used when seeking RIPA authorisations, as the Authorised Officer and/or the Head of Financial and Legal Services will reject any alternative forms used.

Directed Surveillance Forms - Appendix 3

Form A Application for Authority to conduct Directed Surveillance
Form B Review of Directed Surveillance Authority
Form C Renewal of Directed Surveillance Authority
Form D Cancellation of Directed Surveillance

CHIS Forms - Appendix 4

Form E	Application for Authority for Conduct and Use of a 'CHIS'
Form F	Review of Conduct and Use of a 'CHIS'
Form G	Renewal of Conduct and Use of a 'CHIS'
Form H	Cancellation of Conduct and Use of a 'CHIS'

The Council is not required to provide the true identity of the CHIS either on the application form or verbally to the JP.

Communications Data Forms - Appendix 5

Form I	Application for Communications Data
Form J	Application for Communications Data - SPOC Rejection Form
Form K	SPOC Log Sheet
Form L	SPOC Officers Report
Form M	Designated Person's Consideration Form: Application for Communications Data
Form N	Notice under Section 22(4) of RIPA
Form O	Cancellation of Notice under Section 22(4) of RIPA – Applicant
Form P	Cancellation of Notice under Section 22(4) of RIPA – SPOC

Under section 23B(2) RIPA there is no requirement to provide information about the Council's application to access Communications Data to:

- Any person to whom the authorisation or notice which is the subject of the application relates; or
- Any such person's legal representatives.

Any boxes not needed on the Form(s) must be clearly marked as being 'NOT APPLICABLE', 'N/A' or a line must be marked through such sections. Great care must also be taken to ensure accurate information is used and is 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.

Particular care must be taken when considering and confirming whether the proposed surveillance is proportionate to what it seeks to achieve. The explanation must be full and complete.

4. Grounds for Authorisation

Directed Surveillance **(Forms A-D)** or the Conduct and Use of the CHIS **(Forms E-H**) can only be authorised by the Council where an Authorised Officer believes that the authorisation is necessary and proportionate for the purpose of preventing or detecting crime or preventing disorder.

5. Applying for Authorisation

A full description of the proposed surveillance operation must be stated on the relevant Form. Plans should be provided, where possible, and appended to

the form, particularly where camera surveillance is also authorised. Care must also be taken to ensure that a full description of the surveillance operation is given on the authorisation Form.

The use of "cut and paste" entries on Authorisations is not advised as whilst an Officer could exercise careful attention to detail, accuracy and pertinence, there is a small possibility that judicial approval could be refused in the event that the authorisation form is inaccurate.

Investigating and Authorised Officers should assess the *expiry date* (date for cancellation) for an authorisation (following judicial approval). For example, for Directed Surveillance the authorisation is valid for three months and so if the authorisation commences on 01 March, the expiry date is 31 May and not 01 June.

6. Assessing the Application Form

A. Before an Authorised Officer signs a RIPA Form, he or **she must:**

(i) be mindful of this Corporate Policy & Procedures Document, the training provided and any other guidance issued, from time to time, by the Senior Responsible Officer and/or Council Solicitor on such matters;
(ii) recognise that he or she should not be responsible for authorising investigations or operations in which they are directly involved. However, it has been recognised that this may, on occasion, be unavoidable, especially in the case of small organisations, or where it is necessary to act urgently. Where an Authorised Officer authorises such an investigation or operation, the Council Secretary and Solicitor should be informed so that the central record of authorisations can be updated and when inspected, this can be drawn to the attention of a Commissioner or Inspector;
(iii) Satisfy his or herself that the RIPA authorisation is:

In accordance with the law;
Necessary in the circumstances of the particular case on the grounds mentioned in paragraph 4 above; **and**
Proportionate to what it seeks to achieve.

Additional Safeguards when Authorising a CHIS

B. 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 this must address health and safety issues through a risk assessment;
(c) consider the likely degree of intrusion of all those potentially affected;

(d) consider any adverse impact on community confidence that may result from the use or conduct or the information obtained; and
(e) ensure **records** contain particulars and are not available except on a need to know basis.

The Council is not required to provide the true identity of the CHIS either on the application form or verbally to the JP.

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

C. In assessing whether or not the proposed surveillance is proportionate, consider:

(i) the seriousness of the matter giving rise to the proposed surveillance and the importance of taking action in respect of it;
(ii) the implications of not gathering information about the matter;
(iii) the effects of the proposed surveillance on the subject of the surveillance and on other persons;
(iv) compare such effects against the seriousness of the matter and the implications of not taking action;
(v) indicating what, if any, other action instead of that proposed, might be taken; and
(vi) confirming whether the action proposed is likely to be the most effective and the least intrusive means of obtaining the required information.

D. Take into account the risk of intrusion into the privacy of persons other then the specified subject of the surveillance **(Collateral Intrusion**). Measures must be taken, wherever practicable, to avoid or minimise as far as is possible Collateral Intrusion which may assist in determining proportionality;

Authorised Officers, in giving approval, must state on the form, in detail, why they consider the proposed action to be necessary and proportionate.

E. Ensure Authorisation forms include name and addresses of those individuals identified as being subject of RIPA techniques and where appropriate the location (with plan) of the proposed RIPA activity.

F. When signing Authorisations:

i. Ensure that the date and time of signature are included;
ii. Check that a higher level of authority is not required (e.g. where the RIPA technique may acquire confidential information, or a juvenile source or a Vulnerable Individual is engaged as a source).

G. Set a date for review of the internal authorisation and review prior to its expiry to ensure that an application to renew the use of RIPA can be approved by the JP within the expiry date. It is beneficial to review the Authorisation regularly, for example, at least monthly. Put in place

appropriate measures to ensure that the authorisation is appropriately managed..

H. Ensure that the RIPA Departmental Register is duly completed, and that a copy of the RIPA Forms (including any review or cancellation forms) are retained on the departmental file and that the original is forwarded to the Head of Financial and Legal Services **within 1 week of the relevant authorisation, review, renewal, cancellation or rejection**. Copies of the Judicial Approval must also be held on this Register.

I. Mark up the RIPA Departmental Register with the Unique Reference Number (URN) on all pages when the URN is provided by the Head of Financial and Legal Services.

J. Authorised activities, and therefore authorisations, should be regularly reviewed, i.e. at least every 4 weeks.

7. Duration

7.1 The current time limits for an authorisation or notice are:

7.1.1 Three months for Directed Surveillance;
7.1.2 Twelve months for a CHIS (one month if the CHIS is under 18); and
7.1.3 Authorisations and notices for Communications Data 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.

7.2 The grant, renewal and duration of authorisations is set out in section 43 RIPA.

Reviews

7.3 The Forms **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 a maximum of 3 months (from authorisation unless cancelled) for Directed Surveillance (e.g. a Directed Surveillance authorisation granted on 01 April 2005 expires on 30 June 2005) and 12 months (from authorisation) for a CHIS (e.g. a CHIS authorisation granted on 01 April 2005 expires on 31 March 2006).

7.4 However, whether the surveillance is carried out/conducted or not, in the relevant period, does not mean the 'authorisation' is 'spent'. T**he Forms do not expire.** The forms have to be **reviewed and/or cancelled (once they are no longer required).**

~~**Urgent authorisations**~~

~~7.5 Section 43(1) RIPA states that urgent oral authorisation may granted or renewed, which lasts for a period of seventy-two hours. This, however, is~~

~~in limited circumstances, and would not normally be relevant to authorisations for Directed Surveillance and use or conduct of a CHIS where judicial approval is required under section 32A RIPA. Any urgent oral authorisation that is otherwise granted or renewed, 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 (e.g. an urgent authorisation granted at 5.00 pm on 01June expires at 4.59 pm on 04 June).~~

Renewals

7.5 Authorisations can 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.

7.6 The renewal will begin on the day when the authorisation would have expired.

7.7 Applications for renewals should be made just prior to the expiration of the original authorisation. However, the Council must determine the appropriate time to apply for a renewal, but it should be mindful of any matters which may delay the renewal process, for example, intervening weekends or the availability of the Authorised Officer and a JP to grant approval.

7.8 – 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.

Formatted: Indent: Left: 0 cm

7.9 Authorisations may be renewed more than once provided that the use of the technique is considered to be necessary and proportionate.

7.10~~1~~ If during an investigation which has been authorised 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 crime threshold the use of directed surveillance should cease. If Directed Surveillance authorisation is in force it should be cancelled.

Cancellations

7.11~~2~~ Where an Authorised Officer who is satisfied that:

· that it is no longer necessary on the relevant ground of preventing or detecting crime or preventing disorder; and

· the authorisation is no longer proportionate to what is sought to be achieved

he or she must cancel the notice.

7.123 Following approval by the Authorising Officer, the Council's Investigating Officer will need to contact Her Majesty's Courts and Tribunals Service (HMCTS) administration team at the Magistrates' Court to arrange a hearing.

J. Procedure for Judicial Approval

From 01 November 2012, when the Council seeks to authorise the use of Directed surveillance, acquisition of communications data or use of a CHIS under RIPA, it will need to obtain an order approving the grant or renewal of an authorisation or notice from a JP (District Judge or lay Magistrate) before it can take effect.

The hearing will be conducted in private and heard by a single JP who will read and consider the RIPA authorisation and the judicial application. It is only where a JP is satisfied that the statutory tests have been met and that the use of the RIPA technique is necessary and proportionate that an order approving the grant or renewal for the use of the RIPA technique, as described within the application, is issued.

As the hearing at the Magistrates Court is a legal proceeding, the Council officers attending must be formally designated as identified under section 223 of the Local Government Act 1972 and the Council's Standing Orders. It is not the case that only those officers with the skills of legally trained personnel will be required to make the case to the JP.

At the hearing, the Investigating Officer will need to provide the JP with a copy of the original RIPA authorisation and the supporting documents setting out the case and the need to use the RIPA technique. This forms the basis of the application to the JP and should contain all information that is relied upon. It is essential that:

- All of the relevant forms and supporting papers are provided to the JP since these documents form the case;
- Whilst the JP may make notes on the papers during the hearing, the Council must ensure that any information that is fundamental to the case must be submitted on the papers; and
- The Council must ensure that it does not rely on oral evidence that is not reflected or supported within the papers presented at the hearing.

The original RIPA authorisation will record all the relevant information for the RIPA application. Whilst the Council is to provide a brief summary of the circumstances of the case on the judicial application form, this is supplementary and does not replace the need to supply the original RIPA authorisation as well.

The original RIPA authorisation or notice should be shown to the JP but will be retained by the Council so that it is available for inspection by the Commissioners' offices and in the event of any legal challenge or investigations by the Investigatory Powers Tribunal. A copy of the original RIPA authorisation may be taken by the Court.

In addition, the Investigating Officer will provide the JP with a partially completed Judicial application/order. This will be completed by the JP and will form the official record of the JP's decision.
The Investigating Officer will need to obtain judicial approval for all initial RIPA authorisations/applications and renewals and will need to retain a copy of the judicial application/order form after it has been completed and signed by the JP.

There is no requirement for the JP to consider either cancellations or internal reviews.

The Investigating officer to attend the hearing should be the officer who would be able to answer the JP's questions on the policy and practice of conducting covert operations, and provide details of the case itself. It is most likely that the officer will be the case investigator as the officer with the relevant background knowledge of the request and the specific reasons for using a RIPA technique to further the case.

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. The JP will also consider whether there continues to be reasonable grounds.

In addition, the JP must be satisfied that the person who granted the authorisation or gave the notice was an appropriate designated person within the Council and the authorisation was made in accordance with any applicable legal restrictions, for example that the crime threshold for directed surveillance has been met.

Following their consideration of the case the JP will complete the order section of the judicial application/order form recording their decision.

The JP may decide to:

1. **Approve the Grant or renewal of an authorisation or notice - t**he grant or renewal of the RIPA authorisation or notice will then take effect and the Council may proceed to use the technique in that particular case.

2. **Refuse to approve the grant or renewal of an authorisation or notice - t**he RIPA authorisation or notice will not take effect and the Council may not use the technique in that case. If an application is refused the Council should consider the reasons for that refusal and consider whether it can reapply.

3. **Refuse to approve the grant or renewal and quash the authorisation or notice -** A JP may refuse to approve the grant, giving or renewal of an authorisation or notice and decide to quash the original authorisation or notice.

Out of hours access
In the event that the Investigating Officer needs to seek out of hours access to a JP, the Council must follow its local arrangements with the Court staff. In these circumstances, the Council will need to provide two partially completed judicial application/order forms so that one can be retained by the JP. The Council should provide the court with a copy of the signed judicial application/order form the next working day.

Out of hours procedures are for emergencies only and should not be used because a renewal has not been processed in time. 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.

Emergency/ Urgent authorisations
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. An example of an emergency is when criminal activity is observed during routine duties and officers conceal themselves to observe what is happening.

Complaints

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

Committee. In the event that the Council deems it necessary to appeal a JP decision on a point of law, it can only do so by judicial review. The relevant officer must seek legal advice on the merits of such an appeal.

The Independent Powers Tribunal

The Investigatory Powers Tribunal investigates complaints by individuals about a public body's use of RIPA techniques.

If, following a complaint to the Investigatory Powers Tribunal, it finds 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.

The Surveillance Commissioner

The Surveillance Commissioner has an important role in inspecting and monitoring the Council's use of RIPA. It cannot, however, inspect the decision made by the JP as the judiciary is independent.

In the event that the Surveillance Commissioner identifies an error in the authorisation process it will consider the best course of action. This may include asking the Council to cancel the authorisation and, if appropriate, complete a new authorisation taking into account its views and/or concerns which will need to be approved by the JP in the normal way. When an error is brought to the attention of the Council, then it should cease conducting the RIPA activity.

Repeating the process and rectifying errors could result in delay and so it is essential that the authorisation process is followed.

K. Working with or through other agencies

1. If an Officer seeks to utilise the CCTV system operated by the Police a Directed Surveillance Authorisation must be obtained in writing before an approach is made to the "Control Room". In exceptional circumstances, an urgent authorisation may be given orally if the time that would elapse before a written authorisation could be granted would be likely to endanger life or jeopardise the investigation. An urgent authorisation will last no more than 72 hours and must be recorded in writing on the standard form as soon as practicable, with a robust explanation as to why the authorisation was urgent.

2. When another agency has been instructed on behalf of the Council to undertake a RIPA technique, officers must continue to ensure that this document is complied with and its Forms are used. In these circumstances, the Council must inform the agency of its requirements under this document, and the agency must be made explicitly aware what action they are authorised to take.

3. <u>When another agency</u> (e.g. Police, HM Revenue and Customs etc):

   (a) Wishes to use the Council's resources (e.g. CCTV surveillance systems), that agency must use its own internal RIPA procedures. Prior to any agreement to allow the Council's resources to be used for the agency's purposes, Officers should obtain a copy of the agency's RIPA forms for our records (a copy of which must be passed to the **Senior Responsible Officer** to be placed on the Central Register (and/or relevant extracts from the same documents which are sufficient for the purposes of protecting the Council and the use of its resources by such agencies).
   (b) Wishes to use the Council's premises for its own RIPA action, Officers should co-operate with such a request unless there are security or 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 be sought from the other agency, if necessary before the Council co-operates in the agent's RIPA operation. In these circumstances, the Council's own RIPA forms should not be used as the Council is only 'assisting' the RIPA activity of the external agency.

4. If the Police or other Agency wishes to use the Council's resources for general surveillance, rather than specific RIPA operations, they must provide the Council with a written request specifying the proposed use, the extent of remit, the duration, who will be undertaking the general surveillance; and the purpose of seeking to use Council resources.

5. The Council must be satisfied with the written request and purpose of using its resources before any of its resources are made available for the proposed use.

If in doubt, consult with the Senior Responsible Officer at the earliest opportunity.

L. Records Management

1. The Council must keep a detailed record of all Forms, Authorisations, renewals, cancellations and rejections in individual Departments as well as within its Central Register. Such records will include copies of Judicial Approval of the Council's internal Authorisations. The Central Register will be maintained and monitored by the Head of Financial and Legal Services.

Records maintained in the Department

2. The following documents must be retained by the relevant Authorised Officer (or his or her designated Departmental Co-ordinator):

   - a copy of the Forms 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 supporting documentation submitted when the renewal was requested;
   - the date and time when any instruction was given by the Authorised Officer;
   - the Unique Reference Number for the authorisation supplied by the Head of Financial and Legal Services;
   - A copy of the Judicial Approval of the Council's use of RIPA powers.

3. The Head of Financial and Legal Services will issue a Unique Reference Number to Officers, which must be stated on each relevant form.

Information obtained from Directed Surveillance

4. Where material is obtained as a result of Directed Surveillance activities, the Council must make a record of the material. Examples are photographs, video film, surveillance log, and officers' notes.

5. A copy of this record should be given to the Authorised Officer to be filed with the Authorisation Form. The Applicant or Investigating Officer should retain the original on the case file or investigation file.

6. All Officers should ensure that the integrity, security and confidentiality of this material are maintained.

7. Such material should be retained for a period of no more than five years. If the material is no longer required it should, where possible, be destroyed securely on an earlier date. When the material is destroyed, the Council must update the records to state the date of the destruction and the reasons for destruction. The relevant Officer should also sign the record to confirm that the material has been destroyed. A copy of the amended record should then be given to the Authorised Officer.

Records of Use and Product from a CHIS

8. Records of the use and of the materials obtained by a CHIS should be maintained by the Applicant and Authorised Officer. Examples of material are photographs, video film, surveillance log, and officers' notes.

9. A copy of this record should be given to the Authorised Officer to be filed with the Authorisation Form. The Applicant or Investigating Officer should retain the original on the case file or investigation file.

10. All Officers should ensure that the integrity, security and confidentiality of this material are maintained.

11. Such material should be retained for a period of no more than five years. If the material is no longer required it should, where possible, be destroyed securely on an earlier date. When the material is destroyed, the Council must update the records to state the date of the destruction and the reasons for destruction. The relevant Officer should also sign the record to confirm that the material has been destroyed. A copy of the amended record should then be given to the Authorised Officer.

Central Register maintained by Senior Responsible Officer

12. Authorised Officers must forward originals of each Authorisation Form to the Senior Responsible Officer c/o the Council Solicitor for the Central Register, **within 1 week of the authorisation, judicial approval, review, renewal, cancellation or rejection**. The Senior Responsible Officer will monitor the same and give appropriate guidance, from time to time, or amend this Document, as necessary. The Senior Responsible Officer and those authorised by them will have access to the Central Register which will be held in the locked strong room within the Council Solicitor's Department.

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

M. Complaints

1. Copies of the relevant Home Office Guidance and Codes of Practice can be sought from the Home Office website (www.homeoffice.gov.uk). The Council can also provide a copy upon a request from members of the public via the following methods:

   · In writing to The Council Solicitor, Park North, North Street, Horsham, West Sussex, RH12 1RL; or

   · By telephone on 01403 215470.

2. Complaints about the Council's actions under RIPA should be submitted in writing to the Council Solicitor at the above address.

3. Information on the Investigatory Powers Tribunal will be provided as part of the response to any RIPA complaint, including the provision of copies of the Tribunal's complaint form and information leaflet. Alternatively, copies can be sought by contacting the Council Solicitor as set out above.

4. This Corporate Policy and Procedures Document is available on the Council's website at *www.horsham.gov.uk*.