REPORT TO EXECUTIVE

PORTFOLIO AREA: GOVERNANCE & RESOURCES

Date of Meeting: 22 November 2010

Public

Key Decision: No | Recorded in Forward Plan: No

Inside Policy Framework

Title: REGULATION OF INVESTIGATORY POWERS
Report of: Assistant Director (Governance)
Report reference: GD59/10

Summary:
The Report provides an explanation of the Regulation of Investigatory Powers Act (RIPA); makes Members aware of the recent Inspection by the Office of the Surveillance Commissioner; updates and revises the Council's RIPA Protocol; and appraises Members of RIPA usage.

Recommendations:
That the Executive:

i) Note and approve the content of the Report.
ii) Approve the revised Regulation of Investigatory Powers Act Protocol and Guidance Notes as appended to the Report.

Contact Officer: Mark Lambert Ext: 7019

Note: in compliance with section 100d of the Local Government (Access to Information) Act 1985 the report has been prepared in part from the following papers: None

1 Background

1.1 Members are aware that the Council, when carrying out covert surveillance activity, must comply with the Regulation of Investigatory Powers Act (RIPA) 2000 and its associated Regulations and Guidance.

1.2 RIPA provides for public authorities to give authorisation to carry out covert surveillance activities. The term 'public authorities' includes local authorities, therefore, the Council may authorise its officers to carry out covert surveillance.

1.3 The basic premise of RIPA is to ensure that covert surveillance is carried out in the appropriate manner. It requires that the public body wishing to carry out such surveillance does so after carrying out a balancing exercise in which the need for covert surveillance is balanced against the rights of the individual. Article 8 of the Human Rights Act 1998 provides that there shall be no interference with an individual's right to respect for his private and family life other than is necessary in the interests of, inter alia, public safety, the prevention of crime and disorder, the protection of health or morals, or for the protection of the rights and freedoms of others. For covert surveillance to be justified it must be both necessary and proportionate. If it is possible to obtain evidence overtly then this is the method in which it should be gathered.

1.4 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 surveillance are unaware that it is taking place. The definition of surveillance is very wide and includes such activities as:

- Monitoring, observing or listening to persons, their movements their conversations or their other activities or communication;
- Recording anything monitored, observed or listened to in the course of surveillance; and
- Surveillance by or with the assistance of a surveillance device.

It should be noted that Carlisle City Council has never used the powers available to it for the purposes of monitoring any person's private conversations or communications or used any surveillance device that would enable any of these surveillance activities to take place.

Although the term surveillance covers a wide range of activities, it is important to note that RIPA applies only to covert surveillance. If the person who is subject to

the surveillance is aware that it is taking place it will not be necessary to obtain authorisation under RIPA. For example, if someone is believed to be causing a noise nuisance and they are written to and told that they will be monitored then an authorisation will not be necessary.

1.5 The purpose of RIPA is to place covert surveillance activities on a lawful footing. The impetus for this has arisen from the coming into force of the Human Rights Act 1998 ("HRA").

1.6 If a public authority fails to comply with the HRA it is in breach of statutory duty and two possible consequences may follow:

- any person who has suffered loss due to such breach may claim compensation from the public authority; and/or

- any enforcement proceedings brought by a public authority against a person who has suffered such breach may be subject to "collateral challenge" by way of defence of non-compliance by the public authority with the HRA.

1.7 The HRA brings into English Law Article 8 of the European Convention on Human Rights ("Article 8"). This provides that any person is entitled to respect for his private and family life, his home and his correspondence. A public authority should not act in a way which is incompatible with this right; if it does the consequences set out above may flow.

1.8 However Article 8 goes on to provide that there shall be no interference by a public authority with the exercise of the Article 8 right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic wellbeing of the country, for the prevention of disorder or crime, for the protection of health or morals or for the protection of the rights and freedom of others. It is therefore recognised by the Convention that interference with Article 8 rights may sometimes be necessary in order to prevent crime/disorder, protect health etc, such interference must however be on a lawful basis. For the purposes of RIPA, the Council is only able to exercise the power for the prevention of crime and disorder.

1.9 If a Local Authority fails to obtain an authorisation for surveillance in accordance with the scheme set out in the RIPA it has not thereby committed a criminal offence nor is it automatically subject to any sanction or penalty imposed under civil law. However, in the absence of authorisation there is a risk that the Authority will not be

able to demonstrate that any covert surveillance has been carried out on a lawful basis. There then arises the further risk that any proceedings which the Authority is then undertaking against the person concerned (e.g. statutory enforcement proceedings or a prosecution) may be subject to a successful challenge and/or the Authority may be subject to a legal claim for compensation by the person concerned.

1.10 The Council has operated in accordance with the legislation since its inception. Every three years the Office of the Surveillance Commissioner carries out a detailed inspection of the procedures operated by the Council in respect of RIPA. The most recent inspection took place earlier this year.

2 INSPECTION REPORT

2.1 In January 2010 the Council was subject to an inspection by Assistant Surveillance Commissioner, His Honour Norman Jones QC. A copy of the Inspection Report is attached as Appendix 1. There are a number of helpful recommendations made within the Report subject to the caveat that "[s]uch suggestions as can be made are designed to improve only that which is already compliant".

2.2 Members will be pleased to note that the Inspection Report Concludes that "[Carlisle City Council] is an excellent RIPA performing local authority and this Inspection is pleased to endorse the comments made by the last Inspection that this is one of the better performing local authorities in the UK".

3 OPERATIONAL PROTOCOL AMENDMENTS

3.1 Members will see from the Inspection Report that there are a number of amendments. These have all been implemented and the Council's protocol amended accordingly. Members' attention is particularly drawn to the change in officers authorised to approve requests for RIPA authorisation. In accordance with the Inspection Report the number has been reduced from 15 to 5 (with the Town Clerk and Chief Executive being the authorising officer for the use of a juvenile or vulnerable covert human intelligence source (i.e. information obtained by a human relationship) or the acquisition of confidential information).

3.2 The Council's Assistant Directors of Community Engagement, Local Environment and Economic Development are authorised as are two heads of service from the shared Revenues and Benefits Services (the primary users of the power). The Assistant Director (Governance) acts as the RIPA Monitoring Officer with the Legal Services Manager acting as Deputy.

3.3 Members will see that the Inspector also looked at the Council's CCTV system and recommended that an operational protocol should be in place between the Council and Cumbria Constabulary to cater for use they may wish to make of the system. A protocol has been drafted and this is currently with Cumbria Constabulary for their consideration.

3.4 The revised and updated RIPA procedure protocol is shown at Appendix 2.

4 TRAINING

4.1 RIPA training will form part of the Council's Ethical Governance Training Programme. All officers applying for and those authorising surveillance will be trained and also receive refresher training on an occasional yet ongoing basis.

5 PERFORMANCE

5.1 It is important that Members are content that the Council operates its RIPA system properly and it is good practice to report on an annual basis to Members. This is the first report of this nature.

5.2 Members will be aware that there is often comment made about local authorities' misuse of the powers available under RIPA. They should be assured that Carlisle City Council only uses the powers when they are necessary and proportionate. Appendix 3 shows the statistics of the City Council's usage from the inception of the legislation and these show that the powers have only been used twice in 2010; once for directed surveillance and once for a covert human intelligence source (the latter simply being an authorisation for an officer to ring an advertised telephone number and ask for the address of a potentially illegal tattoo party). The predominant use of the powers relates to the investigation of benefit fraud and this only amounts to 41 times in the ten year period. Combined with other surveillance the Council has authorised 63 surveillance activities since 2000. Such surveillance has always been directed and never intrusive and has always been necessary and proportionate.

6 CONSULTATION

None.

7 RECOMMENDATIONS

That the Executive:

iii) Note and approve the content of the Report.

iv) Approve the revised Regulation of Investigatory Powers Act Protocol and Guidance Notes as appended to the Report.

8 REASONS FOR RECOMMENDATIONS

To advise Members of the RIPA processing procedures operating within the Council and to update the Council's RIPA protocol.

9 IMPLICATIONS

- Staffing/Resources – None
- Financial – None
- Legal – The Assistant Director (Governance) has written the Report. The RIPA protocol is an operational document and, therefore, does not fall within the Council's Budget and Policy Framework.
- Corporate – It is important that the Council complies with the obligations placed on it to conduct its affairs properly.
- Risk Management – Failure to comply with the RIPA procedures could jeopardise legal proceedings entered into by the Council.
- Environmental – None.
- Crime and Disorder – The Council may only authorise surveillance if it is for the prevention of crime and disorder.
- Impact on Customers – This report will not change the impact upon customers of the RIPA legislation but the Protocol and approved way in which the Council operates the RIPA regime ensures that any impact is necessary and proportionate as permitted by the legislation.
- Equality and Diversity –

Impact assessments

Does the change have an impact on the following?

Equality Impact Screening	Impact Yes/No?	Is the impact positive or negative?

Does the policy/service impact on the following?		
Age	No	
Disability	No	
Race	No	
Gender/ Transgender	No	
Sexual Orientation	No	
Religion or belief	No	
Human Rights	Yes	Positive
Social exclusion	No	
Health inequalities	No	
Rurality	No	

If you consider there is either no impact or no negative impact, please give reasons:

.....
.....
.....

If an equality Impact is necessary, please contact the P&P team.

The Rt Hon. Sir Christopher Rose

Office of Surveillance Commissioners

Chief
Surveillance
Commissioner

Restricted

18th February 2010

Dear M/s Mooney,

Covert Surveillance

On 27th January 2010, an Assistant Surveillance Commissioner, HH Norman Jones QC, visited your Council on my behalf to review your management of covert activities. I am grateful to you for the facilities afforded for the inspection.

I enclose a copy of Mr Jones's report which I endorse. I am pleased to see that you continue diligently to achieve RIPA compliance and your practices are described by Mr Jones as being "of the highest order" Mr Lambert and M/s Liddle are particularly worthy of commendation.

The recommendations, which are directed to fine tuning, are that authorising officers should be reduced in number, RIPA trained and all required to provide some authorisations, that your Policy and Guidance Notes should be amended as indicated in para 19 of the report, that a protocol be drafted and entered into for covert use of your CCTV system by the police and a suitably redacted copy of the authorisation seen, always, by Council CCTV operators.

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

One of the main functions of review is to enable public authorities to improve their understanding and conduct of covert activities. I hope your Council finds this process constructive. Please let this Office know if it can help at any time.

Yours sincerely

M/s Maggie Mooney
Town Clerk and Chief Executive
Carlisle City Council
Civic Centre
Carlisle CA3 8QG

PO Box 29105 London SW1V 1RB Tel 020 7035 0074 Fax 020 7035 3114
Web: www.surveillancecommissioners.gov.uk email:oscmailbox@osc.gsi.gov.uk

OFFICE OF SURVEILLANCE COMMISSIONERS

INSPECTION REPORT

CARLISLE CITY COUNCIL
27 January 2010

Assistant Surveillance Commissioner:
His Honour Norman Jones

DISCLAIMER

This report contains the observations and recommendations identified by an individual surveillance inspector, or team of surveillance inspectors, during an inspection of the specified public authority conducted on behalf of the Chief Surveillance Commissioner.

The inspection was limited by time and could only sample a small proportion of covert activity in order to make a subjective assessment of compliance. Failure to raise issues in this report should not automatically be construed as endorsement of the unreported practices.

The advice and guidance provided by the inspector(s) during the inspection could only reflect the inspectors' subjective opinion and does not constitute an endorsed judicial interpretation of the legislation. Fundamental changes to practices or procedures should not be implemented unless and until the recommendations in this report are endorsed by the Chief Surveillance Commissioner.

The report is sent only to the recipient of the Chief Surveillance Commissioner's letter (normally the Chief Officer of the authority inspected). Copies of the report, or extracts of it, may be distributed at the recipient's discretion but the version received under the covering letter should remain intact as the master version. Distribution beyond the recipient's own authority is permissible but it is requested that the 'Secretary to OSC', Office of Surveillance Commissioners, is informed of the named individuals to whom copies or extracts have been sent. Any references to it, or extracts from it, must be placed in the correct context.

The Office of Surveillance Commissioners (OSC) is not a public body listed under the FOI Act 2000, however, requests for the disclosure to a third party of any information contained within this report should be notified to the Secretary to OSC."

Office of Surveillance Commissioners

OSC/INSP/075

Chief Surveillance Commissioner,
Office of Surveillance Commissioners,
PO Box 29105,
London,
SW1V 1ZU.

5th February 2010.

INSPECTION REPORT
CARLISLE CITY COUNCIL

Inspection — 27th January 2010.

Inspector — His Honour Norman Jones QC.
Assistant Commissioner

Carlisle City Council.

1. Carlisle City is the most northern City in England. The Council boundaries embrace some 402 square miles of Cumbrian territory and stretch to the Scottish border. It includes the smaller towns of Brampton and Longtown as well as outlying villages including Dalston, Scotby and Wetheral. The city has a population of 100,739.

2. The Senior Corporate Management Structure is headed by the Chief Executive, Ms. Maggie Mooney, who was in post at the time of the last OSC inspection. Two Strategic Directors report to her who are in turn supported by five Assistant Directors. The Council is presently undergoing a period of reorganisation.

3. The Council was last inspected in January 2007 by Mr. Richard Allsopp, Surveillance Inspector. He reported that *this inspection found a vast improvement in the way the Carlisle City Council is now managing its covert surveillance operations. On the strength of the findings of this inspection it is now assessed as one of the better performing public authorities in respect of RIPA.*

4. The Council continues to be a limited user of *RIPA* having granted 18 authorisations since the last inspection. They are predominantly (80%) for benefit fraud investigations with a small number relating to licensing. All were justified. None were *urgent,* concerned *confidential information,* were self authorised or were for the employment of *Covert Human Intelligence Sources (CHIS).*

5. The Council headquarters is at The Civic Centre, Rickergate, Carlisle, CA3 8QG.

Inspection.

6. The Inspection was warmly welcomed by Mr. Mark Lambert, Assistant Director (Governance) who is the Council Solicitor and Monitoring Officer. He is also the *RIPA* Monitoring Officer for the Council. He introduced Ms. Claire Liddle, Principal Solicitor and *de facto* Deputy *RIPA* Monitoring Officer. The inspection was later joined by Ms. Elaine Turner, Revenue and Benefits Manager and authorising officer for her department. In consequence most authorisations for the Council are undertaken by her.

7. The inspection was conducted by means of discussion and interview with the officers. Progress on previous recommendations was discussed followed by consideration of the structure of *RIPA* management, the role and number of authorising officers, the Council *RIPA* training programme and its *RIPA* policy and procedures. This was followed by an examination of Central Record of authorisations and of about half of the retained applications/authorisations, reviews, renewals and cancellations. A short feedback of the findings of the Inspection was conducted with the officers, and the inspection was completed with a visit to the CCTV Control Centre.

8. The Inspection expresses its gratitude to Mr. Lambert and Ms. Liddle for the assistance they afforded it, and for their enthusiastic participation.

Previous recommendations.

9. Two recommendations featured in the last OSC Report:

   I. *The Council's RIPA Policy and Guidance Note and its central record would be even further improved by attention to the matters raised in this report.*

   Following the last inspection amendments were made to the *Guidance Note* in accordance with the advice tendered in the report. In addition a spreadsheet format was introduced as the Central Record matrix. This not only expands as a spreadsheet but also may be printed out in a database format. All topics required by the *Code of Practice for Covert Surveillance* are included except self authorisation. Mr. Lambert confirmed that that addition will be made forthwith. <u>This recommendation has been discharged</u>.

   II. *Refresher training should be undertaken by those members of staff involved in applying for or authorising Directed*

Surveillance. As part of the curriculum, the minor imperfections found in the authorisations inspected during this visit should be highlighted and addressed.

This has been addressed by internal training and by one officer a year being sent on a dedicated *RIPA* course conducted by an external trainer. In addition Mr. Lambert has a dedicated review procedure which involves him considering thoroughly each application/authorisation and ancillary document at the time of, or shortly after, its submission to him. Documents submitted from new authorising officers or from officers who rarely authorise are given particularly close scrutiny. Weaknesses identified are then considered with the relevant officer. This recommendation has been discharged.

***RIPA* management structure.**

10. The Inspection was gratified to understand from the RIPA Monitoring Officer that consideration had been given to the best structure for managing *RIPA* within the Council. The structure devised cannot be faulted. It is operated and controlled centrally by the *RIPA* Monitoring Officer.
    i. He receives original *RIPA* documents from authorising officers and immediately transfers the required detail onto the Central Record matrix and files the documents.
    ii. Oversight is exercised by him considering each document at that stage and referring back any with which he is not happy. Thereafter he conducts a further monthly review of the documents and considers the progress of the authorisation. Where amendments are required it is his practice to require cancellation of the authorisation and its reissue in its amended form.
    iii. He organises training which has been carried out as indicated above (paragraph 9.ii.), and is proposed as outlined below (see **Training**).
    iv. Mr. Lambert is confident that there is already a high degree of *RIPA* awareness within the Council. This is achieved by raising *RIPA* issues at senior management meetings and then *RIPA* issues are cascaded down to the lower departments. He considers that the degree of training and oversight also heighten awareness. However he is contented to adopt further methods such as the distribution of a *RIPA* leaflet and the dissemination of *RIPA* material through Council publications and its intranet.

11. This appears to be an ideal structure for the control of *RIPA* processes within the Council. If any improvement were to be contemplated it lies in the fourth head of raising *RIPA* awareness by adopting the proposed additional methods of dissemination of *RIPA* information. This has importance because it is by ensuring a high degree of *RIPA* awareness throughout the Council that unauthorised

surveillance is avoided. It is to be noted that in the absence of Mr. Lambert Ms. Liddle assumes the role of *RIPA* Monitoring Officer.

Training

12. A training programme is currently under consideration by the *RIPA* Monitoring Officer which will be put into operation as soon as the current Council management reorganisation is completed. This will consist of regular refresher training for all officers likely to be involved in the *RIPA* process. It has yet to be decided whether this should be conducted "in house" by Mr. Lambert and Ms. Liddle or whether, on the first occasion, an external experienced *RIPA* trainer should be brought in. The regular refreshers are anticipated to occur at 12/18 month intervals.

13. Both Mr. Lambert and Ms. Liddle impress with their knowledge of *RIPA* and are more than competent to conduct refresher training. The proposed programme would appear to be ideally suited to the needs of Carlisle City Council.

Authorising officers

14. Some 15 Council officers are designated *RIPA* authorising officers. Of that number only about three engage in any authorising, and of those the vast majority are undertaken by Ms. Elaine Turner on behalf of the Benefit Fraud department. Others have been undertaken by Mr. Lambert for the Licensing department.

15. This number of authorising officers is excessive. Permitting officers who do not authorise with any regularity to do so is courting the production of poor quality authorisations. Whilst these are likely to be picked up in the excellent oversight and quality control system, nevertheless there is little point in tolerating the risk in the first place.

16. A further problem arises from this structure in that the *RIPA* Monitoring Officer is also an active authorising officer. This means that he is exercising oversight, on occasion, on his own authorisations. Mr. Lambert recognises this conflict and proposes that both he and Ms. Liddle are not authorising officers.

17. The Chief Executive or (in his absence) a Chief Officer are the only officers who may authorise the use of a juvenile or vulnerable *CHIS* or the acquisition of *confidential information*. They require to be *RIPA* trained, but otherwise do not need to be regular authorisers. In addition a total of 4 or 5 authorising officers would fulfil the Council's requirements and permit cover for holidays and sickness. Efforts should be made to ensure that all undertake some authorisations. None should authorise unless adequately trained.

(See recommendation)

Policy and procedures.

18. The Council *Policy and Guidance Notes for Staff* provides a comprehensive guide to the Council *RIPA* process. It is particularly encouraging to note that it contains clear directions about the management of *CHIS,* even though the Council is unlikely to use them, and that important issues are printed in bold. Throughout it advises officers to seek advice if in doubt.

19. A few further amendments may assist and these were discussed with the officers. They include amending:

- the present instruction to authorising officers to submit copy documents to the Assistant Director(Governance) to reflect the current practice of submitting originals;
- references to Assistant Director(Governance) to read *RIPA Monitoring Officer* ;
- by including a section setting out the responsibilities of the *RIPA* Monitoring Officer;
- the list of authorising officers to reflect a lower number who should be named as well as identified by office;
- the definition of *private information* to incorporate *aspects of professional and business life;*
- the reference to *necessity* to embrace a consideration of why it is necessary to use covert surveillance in the investigation;
- the reference to *proportionality to* include the three considerations, viz. Whether the proposed covert surveillance is proportional (a) to the mischief being investigated, and (b) to the degree of likely intrusion on the target and others, and whether other reasonable means of obtaining the evidence have been considered and discounted;
- by inviting officers considering the use of the *urgent* provisions to first consider whether the proposed covert surveillance can be met by the *immediate response* provisions of *Section 26(2)(c) of RIPA*;
- To include the time limit for a juvenile *CHIS* authorisation as 1 month.

(See recommendation)

CCTV

20. The inspection was welcomed at the CCTV Control Centre by Mr. Peter Vincent, CCTV Manager, for whose co-operation and assistance, together with that of Mr. Steve McRonald, operator, the Inspection was most grateful. He informed the Inspection that this was the first OSC inspection received at the CCTV Centre.

21. Carlisle Council has 70 CCTV cameras, 65 of which are situated in the City Centre and 3 in Brampton and 2 in Longtown. They are appropriately signed. 55 are dome cameras and 46 are ptz.. The system has been digital since 2006.

22. The cameras are operated on a 24/7 basis by at least one, and often two operators. All are trained to industry standards.

23. The police only rarely seek access to the system. At one stage before 2000 the police controlled the system overnight but in that year the Council assumed full control. A link exists between the CCTV Control Room and the police Control Room at Penrith whereby an image can be forwarded during an incident, usually at the request of the police. However the Council operator retains control of the relevant camera.

24. The relationship with the police is good, though some problem has been experienced for the obtaining of *RIPA* authorisations when covert surveillance has been requested by the police. At present the only information given by the police is a police *RIPA* number together with an operation number and the identity of the police officer concerned. No *RIPA* protocol exists between the Council and the police for use of the CCTV system for covert surveillance.

25. It is of some concern that Council operators are not being given the details of what is authorised by the *RIPA* authorisations. In such cases it is difficult to see how the operator can be sure that particular surveillance undertaken for the police is covered by the police authorisation, and hence may inadvertently place the Council at risk. This situation requires to be rectified by the production of a police/Council CCTV protocol and by the police providing authorisations, suitably redacted to protect sensitive detail, but which disclose what is actually authorised. In the absence of such authorisation the Council should be reluctant to grant access to their system.

(See recommendation)

26. The Inspection was satisfied that those operating the system were fully aware of the needs of *RIPA*, and it was comforting to note that they were aware of the need to ensure that accidental covert surveillance did not occur.

Conclusions.

27. Carlisle Council is highly conscious of the need to be *RIPA* compliant. It has sought to achieve this with diligence. Those practices set in place and which form the Council's *RIPA* system are of the highest order. Such suggestions as can be made are designed to improve only that which is already compliant.

28. In Mr. Lambert the Council has an officer who is fully familiar with *RIPA* and its regulatory framework. He is the principal architect of the system and deserves due praise for its effectiveness. Ms. Liddle provides excellent support and cover in his absence.

29. Save for some concerns relating to the CCTV system, which can be resolved by appropriate arrangements being agreed with the police, this is an excellent *RIPA* performing local authority and this Inspection is pleased to endorse the comments made by the last Inspection that this is one of the better performing local authorities in the UK.

Recommendations.

30.

I. That the number of authorising officers should be reduced and all who authorise for the Council should be *RIPA* trained. All designated authorising officers should undertake some authorisations. (paragraph 17).
II. That amendments should be made to the Council *Policy and Guidance Notes for Staff.*(paragraph 19)
III. That a protocol should be drafted for the usage of the Council CCTV system by the police for the purposes of covert surveillance, and no use should be made of the CCTV system for such purpose unless a copy of the authorisation, suitably redacted but disclosing what has been authorised, is made available to the Council CCTV operators.. (paragraph 25)

His Honour Norman Jones, QC.
Assistant Surveillance Commissioner.

APPENDIX 2

CARLISLE CITY COUNCIL

REGULATION OF INVESTIGATORY POWERS ACT 2000

PROTOCOL AND GUIDANCE NOTES FOR STAFF RELATING TO SURVEILLANCE AND USE OF COVERT HUMAN INTELLIGENCE SOURCES

CONTENTS

SECTION 1

INTRODUCTION

1.1 The Regulation of Investigatory Powers Act (RIPA) 2000 provides for public authorities to give authorisation to carry out **covert surveillance** activities. Public Authorities include local authorities therefore the Council may itself give authorisation to its officers to carry out covert surveillance.

1.2 The basic premise of RIPA is to ensure that covert surveillance is carried out in the appropriate manner. It requires that the public body wishing to carry out such surveillance does so after carrying out a balancing exercise in which the need for covert surveillance is balanced against the rights of the individual. Article 8 of the Human Rights Act 1998 provides that there shall be no interference with an individual's right to respect for his private and family life other than is necessary in the interests of, inter alia, public safety, the prevention of crime and disorder, the protection of health or morals, or for the protection of the rights and freedoms of others. For covert surveillance to be justified it must be both **necessary** (para 4.2.3) and **proportionate** (para 4.2.5). If it is possible to obtain evidence overtly then this is the method in which it should be gathered.

1.3 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 surveillance are unaware that it is taking place. The definition of surveillance is very wide and includes such activities as :

- Monitoring, observing or listening to persons, their movements their conversations or their other activities or communication;
- Recording anything monitored, observed or listened to in the course of surveillance; and
- Surveillance by or with the assistance of a surveillance device.

Although the term surveillance covers a wide range of activities, it is important to note that RIPA applies only to covert surveillance. If the person who is subject to the covert surveillance is aware that it is taking place it will not be necessary to obtain authorisations under RIPA.

1.4 The purpose of RIPA is to place covert surveillance activities on a lawful footing. The impetus for this has arisen from the coming into force of the Human Rights Act 1998 ("HRA").

1.5 If a public authority fails to comply with the HRA it is in breach of statutory duty and two possible consequences may follow :

- any person who has suffered loss due to such breach may claim compensation from the public authority; and/or

- any enforcement proceedings brought by a public authority against a person who has suffered such breach may be subject to "collateral challenge" by way of defence of non compliance by the public authority with the HRA.

1.6 The HRA brings into English Law Article 8 of the European Convention on Human Rights ("Article 8"). This provides that any person is entitled to respect for his private and family life, his home and his correspondence. A public authority should not act in a way which is incompatible with this right; if it does the consequences set out above may flow.

1.7 However Article 8 goes on to provide that there shall be no interference by a public authority with the exercise of the Article 8 right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic wellbeing of the country, for the prevention of disorder or crime, for the protection of health or morals or for the protection of the rights and freedom of others.

It is therefore recognised by the Convention that interference with Article 8 rights may sometimes be necessary in order to prevent crime/disorder, protect health etc, such interference must however be on a lawful basis.

1.8 In anticipation of the coming into force of the HRA it was recognised that covert surveillance activities were in danger of falling foul of Article 8, even if necessary for the reasons set out in Article 8, if it was not demonstrably carried out on a lawful basis.

1.9 RIPA was therefore passed in order to provide a clear lawful basis for covert surveillance to be carried out by public authorities including :

Security Services
Police
Armed Forces
Customs & Excise
Local Authorities

1.10 RIPA is welcome for local authorities because there are a range of activities which are carried and pursuant to a local authority's statutory duties and powers which may potentially (depending on the facts) engage Article 8 for example :

- Trading Standards enforcement;

- Enforcement of controls over statutory nuisance Under Part III EPA 1990;

- Tenancy enforcement particularly 'neighbour nuisance' and anti social behaviour;

- Benefit fraud investigations;

1.11 RIPA assists by :

- Clarifying what types of covert surveillance may be undertaken by local authorities;

- Providing a scheme for the giving of authorisation.

1.12 If a Local Authority fails to obtain an authorisation for surveillance in accordance with the scheme set out in the RIPA it has not thereby committed a criminal offence nor is it automatically subject to any sanction or penalty imposed under civil law. However, in the absence of authorisation there is a risk that the Authority will not be able to demonstrate that any covert surveillance has been carried out on a lawful basis. There then arises the further risk that any proceedings which the Authority is then undertaking against the person concerned (eg statutory enforcement proceedings or a prosecution) may be subject to a successful challenge and/or the Authority may be subject to a legal claim for compensation by the person concerned.

1.13 In order to provide public authorities with guidance the Home Office has issued various Codes of Guidance. Those which apply to local authority's and therefore to Carlisle City Council are as follows (with cross reference to the relevant appendix to this protocol in brackets):

- Covert Surveillance Code of Practice (Appendix 2) – this contains guidance on Directed Surveillance at Chapter 3;

- Covert Human Intelligence Sources Code of Practice (Appendix 3).

1.14 The Home Office has also provided assistance by developing a comprehensive website for RIPA. The site contains the text of the statute, the statutory instruments, the Codes and various articles, notes papers and other miscellaneous items of interest. The address of the website is www.security.homeoffice.gov.uk/ripa. The Office of the Surveillance Commissioners also has a useful website at www.surveillancecommissioners.gov.uk .

1.15 The purposes of this protocol document are to explain what the Council's procedures are for the authorisation and carrying out of

Directed Surveillance and the use of Covert Human Intelligence Sources and also to provide guidance for staff who are designated as Authorising Officers or who are authorised to carry out Directed Surveillance or to use or act as Covert Human Intelligence Sources.

1.16 This protocol document sets out the key concepts which are used in the Act. An understanding of such key concepts is essential for all officers who are designated as Authorising Officers or who are authorised to carry out covert surveillance or who are authorised to use or act as Covert Human Intelligence Sources. It also sets out the procedures for obtaining authorisations and the Council's requirements for record keeping.

1.17 This protocol does not purport to be an authoritative interpretation of the law and is in no way intended to be read in substitution for the RIPA, the Regulations and the Codes of Practice. In the event of any doubt, legal advice should be obtained from the Assistant Director Governance.

1.18 The RIPA Monitoring Officer is responsible for maintaining a centralised record of all authorisations issued by the Council for the carrying out of Directed Surveillance and for the use of Covert Human Intelligence Sources. The records include not only the authorisations themselves but also information relating to reviews, renewals and cancellations.

1.19 It is the responsibility of each Directorate to retain a copy of the authorisations, renewals and cancellations in its own centralised file. A copy should be placed on the individual case file and the original sent to the RIPA Monitoring Officer marked "Confidential".

1.20 Authorisation, Renewal and Cancellation forms are available on request from the RIPA Monitoring Officer or in his absence the Legal Services Manager. Forms will obtained from the Home Office website to ensure that the most up to date forms are used. A link to the relevant forms is provided in Appendix 5.

SECTION 2

WHAT IS AUTHORISED UNDER RIPA?

2.1 This Section of the protocol sets out in very brief terms what is and what is not authorised for Local Authorities under RIPA.

2.2 The words and concepts which are used are defined in Section 3 of this Protocol and reference should be made to that Section in order to obtain a full understanding of the terms used.

2.3 The Council may undertake **"directed surveillance"** if it is properly authorised in accordance with the Act.

2.4 The Council **does not** have any power to authorise the carrying out of **intrusive surveillance**. This can only be authorised by high ranking Police Officers, Customs Officers, Officers of the Armed Forces or the Secretary of State. It is highly unlikely that the Council would ever have the need to undertake intrusive surveillance; only the Secretary of State could authorise the Council to do so. However, as a word of caution, the Council must take care not to carry out intrusive surveillance inadvertently.

2.5 The Council is also empowered under the RIPA to use "**Covert Human Intelligence Sources"**.

2.6 The Council is not empowered to enter on and interfere with property and wireless telegraphy (although some types of public bodies are authorised to do so under the RIPA).

2.7 Authorisations to carry out such surveillance may be given in public authorities by "Authorising Officers". Regulations issued under RIPA provide that the only persons who are entitled to act as Authorising Officers in local authorities are officers at Assistant Chief Officer, Assistant Head of Service, Service Manager or equivalent (see The Regulation of Investigatory Powers) (Directed Surveillance and Covert Human Intelligence Sources) Order 2003 SI 2003/3171.

2.8 The Council has passed resolutions (in accordance with RIPA) setting out which officers in the Council may give authorisations under these powers. A list can be found in the Council's Constitution at Part 3 – Responsibility for Functions Table 2C Designation of "Proper Officers". A copy of the list at the time of writing this Protocol (September 2010) can be found as Appendix 4 – List of Authorising Officers.

SECTION 3

DIRECTED SURVEILLANCE
AND
COVERT USE OF HUMAN INTELLIGENCE SOURCE

3.1 This part of the Protocol describes the concepts of:

- Directed Surveillance;
- Covert Human Intelligence Source.

These terms are used in Part II of RIPA and the Codes.

3.2 **What is "Directed Surveillance"?**

Surveillance is "Directed" for the purposes of RIPA if it is covert, but not intrusive and is undertaken :

(a) for the purposes of a specific investigation or a specific operation;

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

(c) otherwise than by way of an immediate response to events or circumstances the nature of which is such that it would not be reasonably practicable for an authorisation to be sought for the carrying out of the surveillance.

3.2.1 *What is "Surveillance"?*

Under RIPA this is defined to mean:

"(a) monitoring, observing or listening to persons, their movements, their conversations or their other activities or communication;

(b) recording anything monitored, observed or listened to in the course of surveillance; and

(c) surveillance by or with the assistance of a surveillance device."

RIPA states that surveillance does <u>not</u> include :

(a) any conduct of a Covert Human Intelligence Source for obtaining or recording (whether or not using a surveillance

device) any information which is disclosed in the presence of the source; (For example, if you confront a neighbour with evidence obtained by a professional witness or tenant in an attempt to shame them into better behaviour);

(b) the use of a Covert Human Intelligence Source for so obtaining or recording information, or any entry on or interference with property or wireless telegraphy as this would be unlawful unless authorised under warrants for the intelligence service legislation or powers of police and customs officers.

3.2.2 *Is the surveillance covert?*

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.

Whether or not the surveillance is covert is the first question which should be asked when considering the seeking of authorisation; if it is not covert, the framework of the RIPA will not apply. **Overt surveillance should be used whenever possible (paras 4.2.4 and 4.2.5).**

3.2.3 *Is it for the purposes of a specific investigation or a specific operation?*

This may include, for example, an investigation into a complaint relating to anti-social behaviour in relation to the occupants of particular premises, or a complaint relating to noise arising from specific premises or an anti-fraud operation conducted in relation to Housing/Council Tax Benefits.

3.2.4 *Is it in such a manner that is likely to result in the obtaining of private information about a person?*

"Private information" is any information relating to a person in relation to which that person has or may have a reasonable expectation of privacy. This includes information relating to a person's private, family or professional affairs. Private information includes information about any person, not just the subject(s) of an investigation.

For example, if part of an investigation is to observe a member of staff's home to determine their comings and goings then that would be covered. Likewise, the same applies to observation of occupants of premises to record comings and goings of suspected drug dealers or anti-social conduct.

It may also cover the recording of conversations about personal (eg financial/health/sexual life) details by "listening in" or the use of sound recording equipment when monitoring alleged noise nuisance from adjacent premises.

If it is not likely that observations will result in the obtaining of private information about a person, then it is outside the RIPA framework.

3.2.5 *Otherwise than by way of an immediate response to event or circumstances where it is not reasonably practicable to get authorisation*

The Home Office Code gives an example of how a (Police) Officer would not require an authorisation to conceal himself and observe a suspicious person he came across in the course of a patrol.

However, if as a result of an immediate response, a specific investigation subsequently takes place that brings it within the 2000 Act framework.

3.2.6 *Is the Surveillance Intrusive?*

Directed surveillance becomes Intrusive Surveillance if it:

(a) is carried out in relation to anything taking place on any residential premises or in any private vehicle; and

(b) involves the presence of an individual on the premises or in the vehicle or is carried out by means of a surveillance device.

Furthermore, surveillance is intrusive if it is carried out by means of a surveillance device in relation to anything taking place on any residential premises or in any private vehicle but is carried out without that device being present on the premises or in the vehicle, where the device is such that it consistently provides information of the same quality and detail as might be expected to be obtained from a device actually present on the premises or in the vehicle.

If the device is not on the premises or in the vehicle, it is only Intrusive Surveillance if it consistently produces information of the same quality as if it were. This might catch sound recording equipment which is placed in premises next door to the premises which is under investigation.

Commercial premises and vehicles are therefore excluded from intrusive surveillance.

THE COUNCIL IS <u>NOT</u> AUTHORISED TO CARRY OUT INTRUSIVE SURVEILLANCE.

3.3 **Covert use of Human Intelligence Source (CHIS – also known as a "source")**

A person is a source if :

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

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

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

Thus a source may include persons such as agents, informants and officers working undercover.

3.3.1 *Covert purpose*

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

3.3.2 *Covertly uses such a relationship*

A relationship is used covertly, and information obtained as mentioned in 3.4.1(c) above is disclosed covertly, if and only if it is used or, as the case may be, disclosed in a manner that is calculated to ensure that one of the parties is unaware of the use or disclosure in question.

3.3.3 *Information*

It is not clear from the Act whether "information" means only "private information". The inference is there, but it is not expressly stated in the RIPA.

If in doubt it is safer to obtain authorisation.

SECTION 4

AUTHORISATIONS, RENEWALS AND DURATION ETC

4.1 How is authorisation obtained?

4.1.1 As stated above, authorisation may be given by Authorising Officers for:

- Directed Surveillance;
- Covert Use of Human Intelligence Sources.

4.1.2 The person seeking an Authorisation should complete the relevant Authorisation form which should be obtained from the Head of Legal Services or in his absence the Principal Solicitor. A link to the relvant forms is provided in Appendix 5. Having completed the form he should then take it to the Authorising Officer. In order to provide as full information as possible to enable the Authorising Officer to make a fully informed decision, detailed information should be given in the forms regarding "necessary" and "proportionality" (see paragraphs 4.2.2 and 4.2.3 below). Details of what information should be included in the application form are given at paragraph 4.2.8 below.

4.1.3 The Authorising Officer must take the following steps when considering whether or not to give an Authorisation:

- consider if Authorisation is necessary

  (This is explained in paragraph 4.2.2 below);

- Consider if what will be carried out is proportionate to what is sought to be achieved by carrying it out;

  (This is explained in paragraph 4.2.3 below)

- Is there sufficient information in the form? Has it been completed correctly? What must be recorded in the application form in respect of Directed Surveillance is explained at paragraph 4.2.7 below, and in the case of Covert Use of Human Intelligence Sources in paragraph 4.3.2 below;

- Consider potential for collateral intrusion, the steps that may be taken to minimise it and whether a separate authorisation is required. This is explained in paragraphs 4.2.6, 4.2.8 and 4.3.6

below; in the case of Use of a Covert Human Intelligence Source consider arrangements for safety and welfare of the source; before authorisation, a risk assessment should be undertaken - see paragraph 4.3.5;

- Consider any adverse impact on community confidence that might flow from the authorisation. Sensibilities in the local community should be considered where the surveillance is taking place; consider also activities being undertaken by other public authorities which could impact upon the deployment of surveillance; consider the circumstances where the subject of the surveillance might expect a high degree of privacy (eg in the home or where there are special sensitivities).

4.1.4 If the Authorising Officer is satisfied that Authorisation should be given, he should obtain the reference number from the Head of Legal Services. He should then sign the form, record the date and time that the Authorisation is given, and endorse the reference number on the form. He should send the original of the form to the RIPA Monitoring Officer(who is responsible for maintaining the Central Register for the whole Council) in a sealed envelope marked "Confidential", keep a copy in his own Department's central file of Authorisations and place a copy on the case file.

4.2 **The Conditions for Authorisation - Directed Surveillance**

4.2.1 For Directed Surveillance no officer shall grant an authorisation for the carrying out of directed surveillance unless he believes :

(a) that an authorisation is necessary (on the ground detailed below); and

(b) the authorised surveillance is proportionate to what is sought to be achieved by carrying it out.

4.2.2 An authorisation is **necessary** if it is for the purpose of preventing or detecting crime or of preventing disorder;

4.2.3 Significant consideration must be given to the issue of **necessity**. Everyone has the right to respect for his private and family life (Article 8, Human Rights Act 1998). There shall be no interference with this right other than is necessary in the interests of, inter alia, public safety, the prevention of crime and disorder, the protection of health or morals, or for the protection of the rights and freedoms of others. “Necessity” has to be established on the facts of each individual case before an individual’s rights of privacy can be legitimately infringed. Consideration must be given as to why it is necessary to use covert surveillance in the investigation.

4.2.4 Section 80 of RIPA provides a general saving for lawful conduct, i.e. if the conduct in question does not require authorisation under the Act and is lawful in any event then it continues to be lawful. The effect of this section is that if the Council's duty can be carried out without recourse to an authorisation then that is the preferred way to do it. In other words, if the required information can be obtained by overt means in any given circumstance, covert surveillance can never be necessary. The authorisation forms contain a section in which the applicant is required to identify why covert surveillance is necessary in any given case. **It is the task of the authorising officer to apply his mind to this, as well as proportionality, before granting an authorisation.**

4.2.5 In addition the authorisation for the activity must be **proportionate**. This involves a balancing exercise of the need for the activity in operational terms against the degree of interference with the rights of the subject of the surveillance and of any other persons. It will not be proportionate if the interference is excessive in the circumstances of the case or if the information could have been obtained using less intrusive means. All activity must be carefully managed and must not be arbitrary or unfair. When assessing proportionality, consideration must be given to whether the proposed covert surveillance is proportional:

a) To the mischief being investigated;
b) To the degree of likely intrusion on the target and others; and
c) Whether other reasonable means of obtaining the evidence have been considered and discounted.

4.2.6 The onus is therefore on the **Authorising Officer** who is considering an application to authorise such surveillance to be satisfied that it is:

(a) necessary for the ground stated above and;

(b) is proportionate to its aim.

4.2.7 The **conduct** that is authorised by an authorisation is any conduct which

(a) consists of the carrying out of Directed Surveillance of any such description as is specified in the authorisation; and

(b) is carried out in the circumstances specified in the authorisation and for the purposes of the investigation or operation specified or described in the authorisation.

It therefore follows that if Directed Surveillance that is actually

conducted is other than that specified in the authorisation and/or is carried out in circumstances other than those so specified, and/or for a purpose other than that so specified, it will be unauthorised and unlawful. Careful thought should therefore be given when framing an application for authorisation as to the:

- scope of the directed surveillance;

- the circumstances in which it shall be conducted;

- the purpose of the investigation.

The wider the scope of this authorisation the easier it will be to demonstrate that the activities fell within it. On the other hand, it should not be drafted so widely as to be meaningless!

It is also sensible to make any authorisation sufficiently wide enough to cover all the measures required as well as being able to prove effective monitoring of what is done against what is authorised.

4.2.8 Consideration should be given as to whether there is any possibility that **collateral intrusion** may occur. Collateral intrusion is when the privacy of persons who are other than the subject/s of the investigation/operation is impinged upon. Wherever possible steps should be taken to minimise interference in the lives of persons who are not subject(s) of the investigation. An application for authorisation should therefore include an assessment of the risk of collateral intrusion. If anticipated, the potential for intrusion of this type should be minimised. The ongoing possibility for collateral intrusion should be monitored by the Authorising Officer, such monitoring should form part of the continuing review process to which authorisations are subject. The potential for collateral intrusion may be significant enough to warrant refusal of the application for authorisation. If, during the course of an investigation/operation, the privacy of persons other than the subjects of the investigation/operation are unexpectedly interfered with, this should be reported to the Authorising Officer and he should consider whether the original authorisation should be amended or whether a separate authorisation is required.

4.2.9 **Collateral intrusion** is perhaps the most important aspect of proportionality because it constitutes an invasion of the privacy of persons who are not the target of the surveillance who may not be connected in anyway to the ongoing investigation and are probably entirely innocent.

4.2.10 Authorisations shall be given in **writing** by the Authorising Officer except in cases of urgency where they may be given orally. In urgent cases, a statement that the Authorising Officer has expressly authorised the action shall be recorded in writing by the person to

whom the Authorising Officer spoke. Thereafter, as soon as practicable it shall be endorsed by the Authorising Officer. Authorising Officers should not generally be responsible for authorising their own activities but exceptionally this might be unavoidable.

4.2.11 A written application for Directed Surveillance should record:

- the reasons why the authorisation is necessary and on the ground specified in paragraph 4.2.2 (i.e. for the purpose of preventing or detecting crime or preventing disorder);
- why the Directed Surveillance is considered to be proportionate to what it seeks to achieve;
- the identities, where known, of those to be the subject of directed surveillance;
- the nature of the surveillance;
- level of authority required (or recommended where that is different);
- an explanation of the information which it is desired to obtain as a result of the authorisation;
- the details of any potential for collateral intrusion and why it is justified;
- the details any confidential material which is likely to be obtained

and subsequently record whether authority was given or refused, by whom and the time and date.

Additionally, in urgent cases, a written application should record (as the case may be):

- reasons why the Authorising Officer or the Officer certified to act in urgent cases considered the case so urgent than an oral instead of a written authorisation was given; and/or;
- reasons why the person entitled to act in urgent cases considered that it was not reasonably practicable for the authorisation to be considered by the Authorising Officer.

Where the application is oral, the detail referred to above should be recorded in writing as soon as reasonably practicable.

YOU ARE RECOMMENDED TO SEEK ADVICE FROM THE LEGAL SERVICES UNIT WHEN CONSIDERING ANY APPLICATION FOR A CHIS AUTHORISATION OR ANY MATTER RELATED THERETO

4.3 **Conditions for Authorisation - Covert Use of Human Intelligence Sources**

4.3.1 The Authorising Officer must be satisfied that the use of a Covert Human Intelligence Source is necessary and proportionate. In these respects the principles set out in paragraphs 4.2.1 to 4.2.4 inclusive should be applied. Authorisations should be given in writing as described in paragraph 4.2.7 above and Authorising Officers should not be responsible for authorising their own activities eg acting as source or tasking a source save exceptionally where this would otherwise be unavoidable.

4.3.2 An application for the use or conduct of a source should record:

- details of the purpose for which the source will be tasked or deployed (eg in relation to anti-social behaviour);
- the grounds on which authorisation is sought (eg for the purpose of preventing or detecting crime or preventing disorder);
- where a specific investigation or operation is involved, details of that investigation or operation;
- details of what the source will be tasked to do;
- details of the level of authority required (or recommended, where that is different);
- details of potential collateral intrusion;
- details of any confidential material that might be obtained as a consequence of the authorisation.

4.3.3 The conduct so authorised is any conduct that :

(a) is comprised in any such activities involving conduct of a Covert Human Intelligence Source, or the use of a Covert Human Intelligence Source, 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 Covert Human Intelligence Source the authorisation relates; and

(c) is carried out for the purposes of, or in connection with, the investigation or operation so specified or described.

4.3.4 Nothing in the 2000 Act prevents material obtained from the use or conduct of the source being used in evidence in Court proceedings. Existing Court discretion and procedures can protect, where appropriate, the disclosure of the source's identity.

4.3.5 The Authorising Officer must consider the safety and welfare of that source, and the foreseeable consequences to others of the tasks they are asked to carry out. A **risk assessment** should be carried out before authorisation is given. Consideration for the safety and welfare of the source, even after cancellation of the authorisation, should also be considered.

4.3.6 Before authorising the use or conduct of a source, the Authorising officer should believe that the conduct/use including the likely degree of **intrusion** into the privacy of those potentially affected is proportionate to what the use or conduct of the source seeks to achieve. He should also take into account the risk of intrusion into the privacy of persons other than those who are directly the subjects of the operation or investigation ("collateral intrusion": for an explanation as to the meaning of this reference should be made to paragraph 4.2.8 above). Measures should be taken, wherever practicable, to avoid unnecessary intrusion into the lives of those not directly connected with the operation.

4.4 Record Keeping in relation to Sources

4.4.1 Accurate and proper recording keeping should be kept about the source and tasks undertaken although the confidentiality of the source must be maintained. Records of all authorisations should be maintained on the Central Register of Authorisations referred to in Section 5 of this Protocol which should contain the following information:

- the authorisation together with any supplementary documentation and notification of the approval given by the Authorising Officer;

- any renewal of an authorisation, together with the supporting documentation submitted when the renewal was requested;

- the reason why the person renewing an authorisation considered it necessary to do so;

- any authorisation which was granted or renewed orally (in an urgent case) and the reason why the case was considered urgent;

- any risk assessment made in relation to the source;

- the circumstances in which tasks were given to the source;

- the value of the source to the investigating authority;

- a record of the results of any reviews of the authorisation;

- the reasons, if any, for not renewing an authorisation;

- the reasons for cancelling an authorisation;

- the date and time when any instruction was given by the Authorising Officer to cease using a source.

These records shall be retained for a period of at least 3 years from the ending of the authorisation.

RIPA provides that an Authorising Officer must not grant an authorisation for the conduct or use of a source unless he believes that there are arrangements in place for ensuring that there is at all times a person with the responsibility for maintaining a record of the use made of the source.

4.4.2 Records should be kept not only of the Authorisation but of the use of the source as well. The records should contain particulars of:-

(a) the identity of the source;

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

(c) the means used within the Council of referring to the source;

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

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

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

(g) where applicable, the relevant investigating authority in relation to the source (other than the authority that is maintaining the records);

(h) the identities of the persons in the relevant investigating authority who, in relation to the source, are discharging or have discharged the responsibilities mentioned in paragraph 4.5.2 of this Protocol where relevant;

(i) the period for which those responsibilities have been discharged by those persons;

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

(k) all contacts or communications between the source and a person acting on behalf of the Council;

(l) the information obtained by the Council by the conduct or use of the source;

(m) the information so obtained which is disseminated by the Council;

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

4.4.3 The records must be maintained in such a way so as to preserve the anonymity of the source and the information provided by the source. The RIPA Monitoring Officershall be responsible for maintaining the Central Register of Authorisations which will include the information referred to in paragraph 4.4.1 relating to Authorisations and the Authorising Officer shall maintain the information referred to in paragraph 4.4.2 above relating to the use of the source.

4.5 Management and Tasking of Sources

4.5.1 The Authorising Officer must ensure that satisfactory arrangements exist for the management of the source and for bringing to his attention any concerns about the personal circumstances of the source in so far as they might affect:

- the validity of the risk assessment;

- the proper conduct of the source operation, and

- the safety and welfare of the source.

Where such information is brought to the attention of the Authorising Officer, he shall determine whether or not the authorisation shall continue.

4.5.2 RIPA requires that the Council in common with other public authorities; ensures that arrangements are in place for the proper management and oversight of sources including:

- an Officer of the Council will have responsibility for dealing with the source on behalf of the Council ("the Dealing Officer"): this person will usually be below the grade of Authorising Officer;

- another Officer shall have general oversight of the use made of the source ("the Oversight Officer").

4.5.3 The Dealing Officer will have day to day responsibility for:

- dealing with the source on behalf of the Council;

- directing the day to day activities of the source;

- recording the information applied by the source; and,

- monitoring the source's security and welfare.

4.5.4. It will always be sensible to give careful consideration to the scope of tasking of the source. Whenever it becomes apparent to the Dealing Officer or the Oversight Officer that unforeseen action has taken place or where it is intended to task the source in a new or significantly greater way, they must refer the proposed tasking to the Authorising Officer who will consider whether a separate authorisation is required.

4.5.5 Whenever the Council deploys a source it should take into account the safety and welfare of the source when carrying out the action which he has been tasked to do. As stated at paragraph 4.3.5 above, before authorising the use or conduct of a source, the Authorising Officer should ensure that a risk assessment has been carried out. The Dealing Officer is responsible for bringing to the attention of the Oversight Officer any concerns about the personal circumstances of the source including the validity of the risk assessment, the conduct of the source and the safety and welfare of the source. Where appropriate these concerns should be considered by the Authorising

Officer who will decide whether or not to allow the authorisation to continue.

4.6 **Limits of Source's Authority**

A source may, in the context of an authorised operation, infiltrate existing criminal activity, or be a party to the commission of criminal offences, within the limits recognised by law. A source who acts beyond these limits will be at risk of prosecution. The need to protect the source cannot alter this principle.

4.7 **Cultivation of a source**

4.7.1 Cultivation is the process of developing a relationship with a potential source, with the intention of:-

- Covertly making a judgement as to his/her likely value as a source of information;

- Covertly determining whether and, if so, the best way in which to propose to the subject that he/she become a source.

4.7.2 It may be necessary to infringe the personal privacy of the potential source in the process of cultivation. In such cases, authorisation is needed for the cultivation process itself, as constituting the conduct (by the person undertaking the cultivation) of a source.

4.8 **Use and conduct of a source**

Authorisation for the use and conduct of a source is required prior to any tasking. Tasking is an assignment given to the source, asking him or her to obtain information, to provide access to information or to otherwise act, incidentally, for the benefit of the relevant public authority. It may involve the source infiltrating existing criminal activity in order to obtain that information.

4.9 **Vulnerable individuals**

Vulnerable individuals should only be authorised to act as source in the most exceptional circumstances. The meaning of the term 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 unable to protect himself against significant harm or exploitation. Only the Chief Executive or in his absence, a Chief Officer may grant an Authorisation for the use of a vulnerable individual.

4.10 **Juvenile sources**

4.10.1 Special safeguards also apply to the authorisation for the use or conduct of juvenile sources; that is sources under the age of 18 years. On no occasion should the use or conduct of a source under 16 years of age be authorised to give information against his or her parents. In other cases, authorisations should not be granted unless:

- A risk assessment has been undertaken as part of the application to deploy a juvenile source, covering the danger of physical injury and the psychological aspects (eg distress) of his or her deployment;

- The risk assessment has been considered by the authorising officer and he has satisfied himself that any risk identified in it have been properly explained and understood, by the source; and

- The authorising officer has given particular consideration as to whether the juvenile is to be tasked to get information from a relative, guardian or any other person who has for the time being assumed responsibility for his welfare and whether the authorisation is justified in the light of that fact.

4.10.2 In addition, juvenile authorisations should not be granted unless the Authorising Officer believes that arrangements exist which will ensure that there will at all times be a person who has responsibility for ensuring that an appropriate adult will be present between any meetings between the authority and a source under 16 years of age. An "Appropriate Adult" is the parent or guardian of the source; any other person who has assumed responsibility for his welfare or in the absence of any of the foregoing any responsible person aged 18 or over who is not a member of nor employed by the Council.

4.10.3 The duration of an Authorisation is **one month** instead of 12 months.

4.10.4 Only the Chief Executive or in his absence a Chief Officer may grant an Authorisation of the use of a juvenile.

4.11 **Seal of Confession**

The draft Home Office codes provided that: no operations will be undertaken in circumstances covered by the Seal of the Confession. However this provision now appears to have been dropped from the approved Codes.

4.12 **Confidential Material**

4.12.1 RIPA does not provide any special protection for 'confidential material'. Briefly "confidential material" has a special meaning under RIPA and comprise any of the following:

- communications subject to legal privilege;
- confidential personal information;
- confidential journalistic material;

For a further explanation of these terms please refer to the definitions section in Appendix 1.

Nevertheless, such material is particularly sensitive, and is subject to additional safeguards under the Home Office codes. In cases where the likely consequence of the conduct of a source would be for any person to acquire knowledge of Confidential Material, the deployment of the source should be subject to special authorisation by the Head of the Paid Service (Town Clerk and Chief Executive) or (in his/her absence) a Chief Officer. Careful attention should be paid to the provisions in the Home Office codes (Chapter 3 of the Covert Surveillance Code of Practice and Chapter 3 of the Covert Human Intelligence sources Code of Practice).

4.12.2 In general, any application for an authorisation which is likely to result in the acquisition of Confidential Material should include an assessment of how likely it is that Confidential Material will be acquired. Special care should be taken where the target of the investigation is likely to be involved in handling Confidential Material. Such applications should only be made in exceptional and compelling circumstances with full regard to the proportionality issues this raises.

4.12.3 The following general principles apply to Confidential Material acquired under Part II authorisations:-

- Those handling material from such operations should be alert to anything which may fall within the definition of Confidential Material. Where there is doubt as to whether the material is confidential, advice should be sought from the RIPA Monitoring Officerbefore further dissemination takes place;
- Furthermore, careful regard should be had to the provisions in the Home Office Codes of Practice relating to confidential material referred to above.
- Confidential Material should not be retained or copied unless it is necessary for a specified purpose;
- Confidential Material should be disseminated only where an appropriate officer (having sought advice from a legal officer) is satisfied that it is necessary for a specific purpose;

- The retention or dissemination of such information should be accompanied by a clear warning of its confidential nature. It should be safeguarded by taking reasonable steps to ensure that there is no possibility of it becoming available, or its content being known, to any person whose possession of it might prejudice any criminal or civil proceedings related to the information.

- Confidential Material should be destroyed as soon as it is no longer necessary to retain it for a specified purpose.

4.13 **Combined authorisations - joint working etc**

4.13.1 In cases of joint working i.e. with other agencies on the same operation, authority for directed surveillance by the Housing Benefit Investigator must be obtained from the Council's Authorising Officers. Authority cannot be granted by the Benefit Authority's Authorising Officers for the actions of Council staff and vice versa. It is possible for one organisation to act as 'principal' and one as 'agent'. The former will issue the authorisation and ensure that the agent is fully aware of the precise terms of the surveillance to be carried out, thus ensuring that the limits imposed by the authorisation on invasion of privacy are observed. An example of the foregoing in practice would be the use of the Council's CCTV system by another department of the Council or an external agency (e.g. the Police). In this example it would be necessary for the CCTV Controller to be cognisant of the extent of directed surveillance to be undertaken through the CCTV cameras consistent with the terms of the authority which has been issued.

4.13.2 Although it is possible to combine two authorisations in one form the Council's practice is for separate forms to be completed to maintain the distinction between Directed Surveillance and the Use of a Covert Human Intelligence Source.

4.14 **Requirements for Urgent Grants**

4.14.1 Authorisations must be given in writing by the Authorising Officer. However, in urgent cases, they may be given orally. In such cases, a statement that the authorising officer has expressly authorised the action should be recorded in writing as soon as is reasonably practicable. This should be done by the person to whom the authorising officer spoke but should later be endorsed by the authorising officer.

4.14.2 A case is not normally to be regarded as urgent unless the time that would elapse before the authorising officer was available to grant the

authorisation would, in the judgement of the person giving the authorisation, be likely to endanger life or jeopardise the investigation or operation for which the authorisation was being given. An authorisation is not to be regarded as urgent where the need for an authorisation has been neglected or the urgency is of the authorising officer's own making.

4.1.4.3 Before determining that the use of the urgency provisions is most appropriate officers should consider whether the proposed covert surveillance can be met by the emergency response provisions of Section 26(2)(c) of RIPA. Covert surveillance that is likely to reveal *private information* about a person but is carried out by way of an immediate response to events such that it is not reasonably practicable to obtain an *authorisation* under the 2000 Act, would not require a directed surveillance *authorisation*. Remember, the 2000 Act is not intended to prevent law enforcement *officer*s fulfilling their legislative functions.

4.15 **Duration/Renewals**

4.15.1 Authorisations lapse, if not renewed:

- within 72 hours if either granted or renewed orally, (or by a person whose authorisation was confined to urgent cases) beginning with the time of the last grant or renewal, or

- 12 months - if in writing/non-urgent - from date of last renewal if it is for the conduct or use of a Covert Human Intelligence Source or

- in all other cases (ie Directed Surveillance) 3 months from the date of their grant or latest renewal.

4.15.2 An authorisation can be renewed at any time before it ceases to have effect by any person entitled to grant a new authorisation in the same terms. (See paragraph 4.15.4 below)

However, for the conduct of a Covert Human Intelligence Source, a person should not renew unless a review has been carried out and that person has considered the results of the review when deciding to renew or not. A review must cover what use has been made of the source, the tasks given to them and information obtained.

4.15.3 Regular reviews should be carried out of all authorisations which have been issued: it is for the Authorising Officer to determine the frequency of reviews to be carried out. Once a review has been conducted the result should be notified in writing to the RIPA Monitoring Officer in order that it may be recorded on the Central Register. In the case of CHIS authorisations, the review should

include the use made of the source, the tasks given to the source and the information obtained from the source. In particular, reviews should be carried out frequently when it is likely that confidential material may be obtained or collateral intrusion may take place.

4.15.4 An authorisation may be reviewed, renewed, before it is due to expire, and such renewal for up to a further 3 months (Directed Surveillance or, 12 months CHIS) if the Authorising Officer considers this to be necessary. An application for renewal, in the case of Directed Surveillance should record:

- whether this is the first renewal or every occasion on which the authorisation has been renewed previously;
- any significant changes to the information in paragraph 4.2.8 (Directed Surveillance) or 4.3.2 (CHIS);
- the reasons why it is necessary to continue with the Directed Surveillance/use of the source;
- the content and value to the investigation or operation of the information so far obtained by the surveillance;
- in the case of a CHIS the use made of the source since the date of the authorisation/renewal the tasks given to him and the information obtained from him;
- the results of regular reviews of the investigation or operation.

Authorisations may be renewed more than once, if necessary, and the renewal should be kept/recorded as part of the central record of authorisations.

4.16 **Cancellations**

The Authorising Officer has a statutory duty to cancel an authorisation once satisfied that the criteria for authorisation of Directed Surveillance or the use or conduct of a source (as appropriate) are no longer satisfied (s45 RIPA). If the Authorising Officer is no longer available the task will fall on the person who has taken over the role of Authorising Officer.

4.17 **Retention and destruction of product**

4.17.1 Authorising Officers are reminded of the guidance relating to the retention and destruction of Confidential Material as described in paragraph 4.12 above.

4.17.2 Authorising Officers are responsible for ensuring that authorisations

undergo timely reviews and are cancelled promptly after Directed Surveillance activity is no longer necessary.

4.17.3 Authorising Officers must ensure that copies of each authorisation are sent to the RIPA Monitoring Officeras described in Section 5 below.

4.17.4 Authorisations for Directed Surveillance or CHIS are to be securely retained by the Authorising Officer, for a period of 3 years from the ending of the Authorisation. Where it is believed that the records could be relevant to pending or future criminal proceedings, they should be retained for a suitable further period, in accordance with established disclosure requirements (eg Civil Procedure Rules; Code of Practice under the Criminal Procedures and Investigations Act (1996)) commensurate to any subsequent review. Once the investigation is closed (bearing in mind cases may be lodged some time after the initial work) the records held by the Directorate should be disposed of in an appropriate manner (eg shredded).

4.17.5 Authorising officers must ensure compliance with the appropriate data protection requirements and the relevant codes of practice in the handling and storage of material. Where material is obtained by Directed Surveillance or through use of a CHIS which is wholly unrelated to a criminal or other investigation or to any person who is the subject of the investigation, and there is no reason to believe it will be relevant to future civil or criminal proceedings, it should be destroyed immediately. Consideration of whether or not unrelated material should be destroyed is the responsibility of the Authorising Officer.

4.17.6 There is nothing in the RIPA that prevents material obtained through the proper use of the authorisation procedures from being used in other investigations. However, the use outside the authority which authorised the surveillance, or the courts, of any material obtained by

means of covert surveillance and, other than in pursuance of the grounds on which it was obtained, should be authorised only in the most exceptional circumstances.

SECTION 5

CENTRAL REGISTER OF AUTHORISATIONS

AND RETENTION REQUIREMENTS

5.1. The Council has a Statutory Monitoring Officer who also fulfils the responsibility of the Council's RIPA Monitoring Officer. As such, the RIPA Monitoring Officer is responsible for the oversight of the Council's RIPA activities, the maintenance of the RIPA Protocol, maintenance of the Central Register of Authorisations. The RIPA Monitoring Officer will ensure that all involved have the appropriate level of training. He or she provides definitive advice for the purposes of RIPA and officers should not hesitate to seek assistance if required. In the absence of the RIPA Monitoring Officer the Deputy Monitoring Officer will also act as Deputy RIPA Monitoring Officer.

5.2 The RIPA requires a central register of all authorisations to be maintained by authorities coming within the Act. The Council's RIPA Monitoring Officer maintains this register.

5.3 Whenever an authorisation is issued (including renewals and when cancellations are issued) the Authorising Officer must forthwith arrange for a the fully detailed Authorisation to be sent to the RIPA Monitoring Officer in a sealed envelope marked "Confidential" and to his Directorates Record holder, with a further copy being placed on the individual case file.

5.4 In addition, the following documentation should be retained, by the Record Holder in the Directorates where authorisation has taken place:

- a copy of the application and a copy of the authorisation together with any supplementary documentation and notification of the approval given by the Authorising Officer;
- a record of the period over which the investigation/surveillance has taken place;
- the frequency of reviews prescribed by the Authorising Officer;
- a record of the result of each review of the authorisation;
- a copy of any renewal of an authorisation, together with the supporting documentation submitted when the renewal was requested;

- the date and time when any instruction was given by the Authorising Officer.

5.5 The RIPA Monitoring Officer or his nominated deputy shall be responsible on a monthly basis for reviewing any outstanding authorisations contained within the Central Register. In particular, the RIPA Monitoring Officer should ascertain whether authorisations have been reviewed or cancelled as appropriate by the relevant Authorising Officer.

5.6 The RIPA Monitoring Officer should signify that the required monthly review has been satisfactorily conducted by signifying to this effect on the review log contained within the Central Register of Authorisations.

SECTION 6

CODES OF PRACTICE

6.1 There are Home Office codes of practice that expand on this guidance and copies are available on the Home Office website or on request from Legal Services.

6.2 The codes do not have the force of statute, but are admissible in evidence in any criminal and civil proceedings. As stated in the codes, "if any provision of the code appears relevant to a question before any Court or tribunal considering any such proceedings, or to the tribunal established under the RIPA , or to one of the commissioners responsible for overseeing the powers conferred by the RIPA, it must be taken into account".

6.3 Staff should refer to the Home Office Codes of Practice via the links in the relevant appendices:-

- Covert Surveillance Code of Practice (Appendix 2) – this contains guidance on Directed Surveillance at Chapter 3;

- Covert Human Intelligence Sources Code of Practice (Appendix 3).

SECTION 7

BENEFITS OF OBTAINING AUTHORISATION UNDER THE 2000 ACT.

7.1 **Authorisation of surveillance and human intelligence sources**

The RIPA states that

- if authorisation confers entitlement to engage in a certain conduct and

- the conduct is in accordance with the authorisation, then

- it shall be "lawful for all purposes".

However, the corollary is not true – i.e. if you do not obtain the RIPA authorisation it does not automatically make any conduct unlawful (e.g. use of intrusive surveillance by local authorities). However, you cannot take advantage of any of the special RIPA benefits and that may entail that any enforcement action taken by the Council following unauthorised conduct may be subject to collateral challenge under the Human Rights Act 1998. Furthermore, if a person can prove that their Article 8 rights have been infringed as a result of unauthorised conduct they may sue the Council and claim compensation.

7.2 The RIPA states that a person shall not be subject to any civil liability in relation to any conduct of his which -

(a) is incidental to any conduct that is lawful by virtue of S27(1); and

(b) is not itself conduct an authorisation or warrant for which is capable of being granted under a relevant enactment and might reasonably be expected to have been sought in the case in question.

SECTION 8

SCRUTINY AND TRIBUNAL

8.1 To effectively "police" RIPA, there is provision for the setting up of Commissioners to provide independent oversight carried out thereunder. It provides for the appointment of a Chief Surveillance Commissioner to keep under review, among others, the exercise and performance by the persons on whom are conferred or imposed, of the powers and duties in Part II. This includes authorising Directed Surveillance and the use of Covert Human Intelligence Sources.

8.2 RIPA also provides for the establishment of a tribunal to consider and determine complaints made under the RIPA. It will be made up of senior members of the legal profession or judiciary and shall be independent of the Government. The Tribunal has full powers to investigate and decide any case within its jurisdiction.

Complaints can be made by persons aggrieved by conduct e.g. Directed Surveillance. The forum hears applications on a judicial review basis. Claims should be brought within one year unless it is just and equitable to extend that.

The tribunal can order, among others, the quashing or cancellation of any warrant or authorisation and can order destruction of any records or information obtained by using a warrant or authorisation or records of information held by any public authority in relation to any person. The Council is, however, under a duty to disclose or provide to the tribunal all documents they require if

- It has granted any authorisations under Part II of the 2000 Act.
- It has engaged in any conduct as a result of the authorisation.
- We hold the rank, office and position in a public authority for whose benefit any such authorisation has been or may be given.

APPENDIX 1

Definitions from the 2000 Act

- "1997 Act" means the Police Act 1997.
  "2000 Act" means the Regulation of Investigatory Powers Act 2000.

- **"Confidential Material"** has the same meaning as it is given in sections 98-100 of the 1997 Act.

  It consists of:-

  (a) matters subject to legal privilege;

  (b) confidential personal information; or

  (c) confidential journalistic material.

- **"Matters subject to legal privilege"** includes both oral and written communications between a professional legal adviser and his/her client or any person representing his/her client, made in connection with the giving of legal advice to the client or in contemplation of legal proceedings and for the purposes of such proceedings, as well as items enclosed with or referred to in such communications. Communications and items held with the intention of furthering a criminal purpose are not matters subject to legal privilege (see Note A below)

- **"Confidential Personal Information"** is information held in confidence concerning an individual (whether living or dead) who can be identified from it, and relating:

  (a) to his/her physical or mental health; or

  (b) to spiritual counselling or other assistance given or to be given, and

  which a person has acquired or created in the course of any trade, business, profession or other occupation, or for the purposes of any paid or unpaid office (see Note B below). It includes both oral and written information and also communications as a result of which personal information is acquired or created. Information is held in confidence if:

  (c) it is held subject to an express or implied undertaking to

hold it in confidence; or

(d) it is subject to a restriction on disclosure or an obligation of secrecy contained in existing or future legislation.

- "**Confidential Journalistic Material"** includes material acquired or created for the purposes of journalism and held subject to an undertaking to hold it in confidence, as well as communications resulting in information being acquired for the purposes of journalism and held subject to such an undertaking.

- "**Covert Surveillance"** means surveillance which is carried out in a manner calculated to ensure that the persons subject to the surveillance are unaware that it is or may be taking place;

- For the purposes of authorising directed surveillance under the 2000
  Act an "authorising officer" means the person designated for the purposes of section 28 of the 2000 Act to grant authorisations for directed surveillance. (see the Regulation of Investigatory Powers
  (Prescription of Offices, Ranks and Positions) Order SI 2000/2417.

- **"Working Day"** means any day other than a Saturday, a Sunday, Christmas Day, Good Friday or a day which is a bank holiday under the Banking and Financial Dealings Act 1971 in any part of the United Kingdom

Note A. *Legally privileged communications will lose their protection if there is evidence, for example, that the professional legal adviser is intending to hold or use them for a criminal purpose; privilege is not lost if a professional legal adviser is properly advising a person who is suspected of having committed a criminal offence. The concept of legal privilege shall apply to the provision of professional legal advice by any agency or organisation.*

Note B. *Confidential personal information might, for example, include consultations between a health professional or a professional counsellor and a patient or client, or information from a patient's medical records.*

APPENDIX 2

COVERT SURVEILLANCE

CODE OF PRACTICE

http://www.homeoffice.gov.uk/counter-terrorism/regulation-investigatory-powers/

APPENDIX 3

COVERT HUMAN INTELLIGENCE SOURCES

CODE OF PRACTICE

http://www.homeoffice.gov.uk/counter-terrorism/regulation-investigatory-powers/

APPENDIX 4

LIST OF AUTHORISING OFFICERS

AUTHORISING OFFICERS

Assistant Director (Local Environment)	Angela Culleton
Assistant Director (Economic Development)	Christopher Hardman
Assistant Director (Resources)	Peter Mason
RBS Shared Services Performance Manager	Elaine Turner
RBS Benefits Manager	Mark Wilson
Town Clerk and Chief Executive (Juvenile or Vulnerable Person CHIS or the acquisition of confidential information.)	Maggie Mooney

APPENDIX 5

AUTHORISATION FORMS

All forms may be found from the following link:

http://www.homeoffice.gov.uk/counter-terrorism/regulation-investigatory-powers/

Note: Carlisle best practice is to obtain the relevant form direct from the RIPA Monitoring Officer to ensure (a) it is the most up to date form and (b) a URN may be allocated.

	Housing	Benefit Fraud	Environmental Health	Licensing	APPENDIX 3
2000	1				
2001	3	6			
2002	2	5	1		
2003		5	3	2	
2004		5	1	1	
2005				1	
2006		1		3	
2007		4			
2008		4		3	
2009		10			
2010		1	1		
Totals	6	41	6	10	63

NB: Housing = Anti Social Behaviour
Env Health = Regulatory Matters - unlicensed tattooing/clean neighbourhoods

2010 Env Health = 1 CHIS for an unlicensed tattoo parlour
All others are Directed Surveillance