Appendix 2

CORPORATE GUIDANCE DOCUMENT

REGULATION OF INVESTIGATORY POWERS ACT 2000

September 2017

C O N T E N TS

Any member of staff requiring parts of this guidance to be made available in a different language or format should contact their Service Diversity Group member representative.

APPENDICES

FOREWORD

1.0 This document addresses the requirements of the Regulation of Investigatory Powers Act 2000 (RIPA) and its codes of practice, in relation to the covert surveillance of individuals, the use of covert human intelligence sources, including undercover officers/agents/informants and the recording of telephone conversations. In addition, procedures for obtaining communications data fall within the Act's remit.

These procedures provide a summary and overview of the legislation and codes of practice. DO NOT seek to rely on them alone. In the event of any doubt, the officer should refer to the relevant legislation or code or contact Legal Services for advice.

1.1 RIPA had effect from 1 October 2000. There are Codes of Practice which impose requirements as regards authorisation procedures and records, which must be followed by Public Authorities undertaking investigations, which fall within the scope of RIPA.

1.2 Durham County Council works almost exclusively with, through and for people. We are, therefore, passionate about the authority's commitment to promoting a just society that gives everyone an equal chance to learn, work and live, free from discrimination and prejudice. This guidance demonstrates our desire to carry out our criminal investigations in a fair and equitable manner that respects all human rights and contributing to this commitment.

1.3 Enforcement activities of the authority which fall within the remit of RIPA are subject to monitoring and oversight by the Office of Surveillance Commissioners and the Interception of Communication Commissioner's Office.

1.4 Staff should therefore familiarise themselves with this document and the Codes of Practice. If in any doubt guidance should be sought before undertaking any activity, which falls within the scope of RIPA.

1.5 Complaints made regarding activities of the Authority, which are within the scope of the RIPA, can be investigated by an independent tribunal.

1.6 Copies of the Codes of Practice are readily available for reference on the Intranet.

1.7 Officers must appreciate that should they fail to follow the requirements of RIPA and Codes of Practice, Durham County Council may be liable to claims alleging breaches of an individual's rights under the Human Rights Act 1998.

1.8 Failure to follow RIPA and its Codes of Practice may also adversely affect the admissibility of any evidence obtained using methods covered by the Act. The safety of members of the public supplying information to the council may also be compromised. Where an authorisation is not in place, it may not be possible to seek exemption from disclosure under the provisions of Public Interest Immunity.

1.9 When undertaking any covert investigation, officers should have regard to the health and safety of persons affected by the activity. This may include themselves, colleagues and members of the public. A suitable and sufficient risk assessment of the investigation technique being proposed should be undertaken, having regard to Durham County Council Corporate Health and Safety Policy and any supplemental guidance issued by individual directorates. This needs to be communicated to all those at risk.

1.10 The monitoring of Internet and e-mail within the Council use is regulated by The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000. The ICT service within the Resources Directorate has software in place to monitor the use of the internet and email. If anomalies are identified, these will be investigated by the Information Security Officer in liaison with Internal Audit.

1.12 A register, which records all of the authority's activities falling within the remit of RIPA, has been prepared and is included within the Central Record which is held by Legal and Democratic Services.

1.13 **The most frequently used RIPA applications forms are available on the Intranet and from the RIPA Monitoring Officer in Legal and Democratic Services. The other forms are available from the RIPA Monitoring Officer.**

DEFINITIONS

Directed Surveillance and Covert Human Intelligence Sources

Authorising Officer	The person(s) designated under Sections 28 and 29 of the Act to grant authorisations for directed surveillance and the use and conduct of a Covert Human Intelligence Source, respectively. Within a Local Authority this is Corporate Director, Head of Service or Service Manager. The Council's Authorising Officers are appointed by the Chief Executive. A list of the Council's Authorising Officers can be found as Appendix 1.
Confidential Material:	Communications subject to legal privilege, communications between a Member of Parliament and another person on constituency matters, confidential personal information or confidential journalistic material.
Covert Human Intelligence Source: (CHIS)	Commonly known as Agents, Informants, Undercover Officers. (NB. See RIPA and the Codes of Practice for the definition).
Covert Surveillance	Surveillance carried out in a manner calculated to ensure that the persons subject to the surveillance are unaware that it is taking place.
Directed Surveillance:	Means surveillance which is covert but not intrusive, is conducted for the purposes of a specific investigation, is likely to result in the obtaining of private information about a person and is conducted 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 under Part II of the Act to be sought.
Intrusive Surveillance:	***In no circumstances is the Council permitted to carry out intrusive surveillance*** Covert surveillance carried out in relation to anything taking place on residential premises or in any private vehicle, that involves the presence of an individual on the premises or in the vehicle or is carried out by means of a surveillance device. Surveillance which 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, is not intrusive unless 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.

RIPA Monitoring Officer	Governance Solicitor and Senior Committee Services Officer who are responsible for maintaining the central register, the oversight of RIPA applications and training.
Private Information	This includes any information relating to a person's private or family life. Private information should be taken generally to include any aspect of a person's private or personal relationship with others, including family and professional or business relationships. Whilst a person may have a reduced expectation of privacy when in a public place, covert surveillance of that person's activities in public may still result in the obtaining of *private information*. This is likely to be the case where that person has a reasonable expectation of privacy even though acting in public and where a record is being made by a *public authority* of that person's activities for future consideration or analysis. Private life considerations are particularly likely to arise if several records are to be analysed together in order to establish, for example, a pattern of behaviour, or if one or more pieces of information (whether or not available in the public domain) are covertly (or in some cases overtly) obtained for the purpose of making a permanent record about a person or for subsequent data processing to generate further information. In such circumstances, the totality of information gleaned may constitute *private information* even if individual records do not. Where such conduct includes surveillance, a directed surveillance *authorisation* may be considered appropriate.
Senior Responsible Officer (SRO):	Head of Legal Services/Monitoring Officer who is responsible for the integrity of the process in place within the authority for surveillance, compliance with Part 2 of RIPA and the Codes of Practice, oversight of reporting errors, engagement with the OSC during and post inspections.
Controller	The person or designated managerial officer responsible for overseeing the use of the source and recording this information.
Handler	An investigating officer having day to day responsibility for: - dealing with the source on behalf of the authority - directing the day to day activities of the source - recording the information supplied by the source - monitoring the security and welfare of the source.

Conduct of a Source	Any action of that source, falling within the terms of the Act, or action incidental to it. (i.e. What they do).
"The Use" of a source	Any action to induce, ask or assist a person engaged in the conduct of a source or to obtain information by means of an action of the source. (What they are asked to do).

Surveillance includes:-

- monitoring, observing or listening to persons, their movements, their conversations, or their activities or communications.

- recording anything monitored, observed or listened to in the course of surveillance.

- surveillance by or with the assistance of a surveillance device (any apparatus designed or adapted for use in surveillance).

Tasking: -

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.

Communications Data

Applicant

This is the officer involved in conducting an investigation or operation who makes an application electronically for the acquisition of communications data.

Communications Service Provider (CSP)

These include telecommunications, Internet (including email) and postal service providers.

Designated Person

This is the authorising officer for the purposes of obtaining communications data who must be registered with the National Anti Fraud Network by the SRO. This person must not be the applicant.

Senior Responsible Officer (SRO)

Head of Legal Services/ Monitoring Officer who is responsible for ensuring that the Applicant, Designated Person or other person makes available to the Single Point of Contact such information as the SRO thinks necessary to ensure the integrity of the process, oversight of reporting errors, engagement with the IOCCO during and post inspections.

Single Point of Contact (SPOC)

The Council processes its RIPA applications for communications data via the National Anti Fraud Network (NAFN). NAFN operates a secure online system for the acquisition of communications data under RIPA. NAFN officers act as Single Points of Contact or SPoCs to ensure that Council applications meet the necessary standards before the application is approved by a Designated Person (DP) who is an officer within the Council.

A. COVERT SURVEILLANCE

1.0 INTRODUCTION

1.1 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.

1.2 A RIPA authorisation provides lawful authority for a Public Authority to carry out covert surveillance.

1.3 The Authorising Officers are documented in the central RIPA record held within Legal and Democratic Services. Where possible, Authorising Officers should not authorise operations in which they are directly involved.

1.4 Whenever covert surveillance takes place and is for the purpose of obtaining, or is likely to obtain private information about a person (whether or not they are the target of the operation) an authorisation should be obtained.

(For exemption see 4.3.)

1.5 By obtaining an authorisation, the surveillance operation is carried out in accordance with the law and the safeguards that exist.

1.6 Prior to granting an authorisation the Authorising Officer must be satisfied that the proposed surveillance is necessary for the prevention of crime and is proportionate to what it seeks to achieve. This involves balancing the seriousness of the intrusion into the privacy of the subject of the operation (or any other person who may be affected) against the need for the activity in investigation and operational terms.

1.7 Careful consideration must also be given to any community sensitivities that may be exacerbated by any individual surveillance operation.

1.8 Before applying for an authorisation, the Investigating Officer should consider whether or not the evidence sought could be obtained by alternative methods.

2.0 COLLATERAL INTRUSION

2.1 The officer seeking the authorisation should also consider the possibility of collateral intrusion. This is private information about persons who are not subjects of the surveillance or property interference activity. Steps should be taken to assess the risk, and where possible minimise the risk of collateral intrusion. Where unforeseen collateral intrusion occurs during an operation, the Authorising Officer must be notified and consideration given to amending the authorisation following a review.

2.2 Consideration must also be given as to whether or not the surveillance activities of the Service take place where similar activities are also being undertaken by another agency e.g. the Police, Benefits Agency, Environment Agency.

2.3 Liaison should also be made with Durham Constabulary Local Intelligence Officers, where appropriate.

3.0 RECORDS OF AUTHORISATIONS

3.1 A record of all authorisations must be maintained for 5 years from the ending of each authorisation. This should include not only those authorisations granted, but also those which are refused.

3.2 A copy of each authorisation will be maintained by the Authorising Officer, within each service. The original authorisation must be supplied to the **central record** of authorisations managed by Legal and Democratic Services.

3.3 Due to the sensitive nature of **all documentation** covered by the Act, consideration **MUST** be given to the means by which original authorisations are forwarded to the central record to ensure confidentiality.

4.0 AUTHORISATIONS FOR DIRECTED SURVEILLANCE

4.1 An authorisation is required for covert surveillance undertaken:

(a) for a specific investigation or operation; and

(b) where the surveillance is likely to result in obtaining private information about any person (whether or not they are the subject of the surveillance).

4.2 An authorisation is **NOT** required for covert surveillance carried out as an immediate response to events or circumstances, which could not be foreseen.

4.3 Authorisations do not cover covert surveillance that is carried out in relation to anything taking place on any residential premises or in any private vehicle and involves the presence of an individual on the premises or in the vehicle or is carried out by means of a surveillance device. This activity is termed as **INTRUSIVE SURVEILLANCE AND CANNOT BE UNDERTAKEN BY LOCAL AUTHORITIES**. An observation post outside of premises with a limited view and no sound would not constitute intrusive surveillance. If equipment is used without being the device being on the premises/ vehicle and consistently provides information of the same quality as if it were on the premises / vehicle the action may qualify as intrusive surveillance. (For further guidance see Section 26 of the Act).

4.4 The use of overt CCTV surveillance systems is not normally caught by the Act, since members of the public are aware that such systems are in use. There may be occasions when public authorities use covert CCTV systems for the purposes of a specific investigation or operation. In such cases, authorisation for directed surveillance may be necessary. A protocol has been produced to protect those officers, responsible for such systems, from being pressured into carrying out covert directed surveillance, without an appropriate authorisation. This protocol is shown in Appendix 3.

4.5 Where the surveillance activity is likely to result in confidential material being obtained, the authorising officer within Durham County Council, will be the Chief Executive, or in his absence, his Deputy.

5.0 COVERT VIDEO CAMERA AND AUDIO RECORDING EQUIPMENT

5.1 This equipment is frequently employed during test purchase exercises and other monitoring activities undertaken by the authority for the purpose of recording the transaction/activity and obtaining photographic evidence of the suspect. Concealed voice recorders may be used to record conversations without the knowledge of the other party.

5.2 The deployment of such equipment clearly has the potential for not only obtaining personal information in relation to the suspect, but also collateral intrusion into the activities of other persons in the vicinity of the operation.

5.3 An authorisation is THEREFORE REQUIRED before using such equipment to safeguard against any challenge as to Human Rights infringements. The manner in which such equipment is used may also invoke the requirements relating to **Covert Human Intelligence Sources and Part B of this Manual should be consulted.**

6.0 GROUNDS FOR AUTHORISING DIRECTED SURVEILLANCE APPLICATIONS

6.1 For an authorisation for directed surveillance it **must** be shown to be necessary to use covert surveillance in the investigation on specific grounds. Directed surveillance undertaken by Local Authorities can only be authorised for the purpose of preventing or detecting criminal offences that are either punishable, whether on summary conviction or indictment, by a maximum term of at least 6 months imprisonment or are related to the underage sale of alcohol and tobacco.

6.2 Directed surveillance cannot be authorised for the purpose of preventing disorder that does not involve criminal offence(s).

7.0 JUDICIAL APPROVAL OF DIRECTED SURVEILLANCE APPLICATIONS

7.1 From 1 November 2012 a local authority who wishes to authorise the use of directed surveillance will need to obtain an order approving the grant or renewal of an authorisation or notice from a Justice of the Peace (a District Judge or Lay Magistrate) before it can take effect. If the Justice of the Peace is satisfied that the statutory tests have been met and that the use of directed surveillance is necessary and proportionate, he/she will issue an order approving the grant or renewal for the use of the technique as described in the application.

Further guidance on the Local Authority judicial application process including the Council's RIPA Authorisation Procedure can be found on the Intranet and from the RIPA Monitoring Officer.

8.0 DURATION OF AUTHORISATION

8.1 A written authorisation is valid for 3 months, unless cancelled. This begins on the day on which the Justice of the Peace approves the grant of the application, the expiry date will be considered to be three months minus one day from the date of signature by the Justice of the Peace. The time at which the authorisation is granted must also be recorded on the documentation.

9.0 RENEWAL

9.1 An authorisation may be renewed for a further period of 3 months. A renewal of a grant of a directed surveillance authorisation must be approved by a Justice of the Peace before it can take place. It may be renewed more than once, provided that the renewal continues to meet the criteria for authorisation. The number of occasions it has been renewed should be recorded. The details of any renewal should be recorded centrally.

10.0 REVIEW

10.1 The Authorising Officer should ensure that a system is in place to review authorisations, before it ceases to have effect. It is a matter for the authorising officer to determine how frequently a review is necessary and practicable. This must be stated within the authorisation as a **control measure.** The authorisation should also be reviewed prior to expiry to determine whether or not a renewal is required and can be justified. The authorising officer may make use of one of the following for example: a diary entry, work planner, MS Exchange calendar/alarm facility to generate a message prompt at least **ten** days before the expiry date.

10.2 The Authorising Officer may amend specific aspects of the authorisation upon a review, for example by discontinuing surveillance against particular persons or the use of particular tactics.

11.0 CANCELLATIONS

11.1 The Authorising Officer who granted or last renewed the authorisation **must** cancel it, if satisfied that the directed surveillance no longer satisfies the criteria upon which it was authorised. Where the Authorising Officer is no longer available, this duty will fall on the person who has taken over the role of Authorising Officer or the person who is acting as Authorising Officer.

11.2 An authorisation should also be cancelled once the activity, which was the subject of the authorisation, has been completed. The authorisation should not be left to lapse as a result of the time limit expiring.

11.3 As soon as the decision is taken that directed surveillance should be discontinued, the applicant or other investigating officer involved in the investigation should inform the Authorising Officer. The Authorising Officer will formally instruct the investigating officer to cease the surveillance, noting the time and date of their decision. This is required for the cancellation form. The date and time when such an instruction was given should also be recorded in

the central record of authorisations. It is also necessary to detail the amount of time spent on the surveillance as this is required to be retained by the SRO.

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

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

11.6 The cancellation form will be filed by the Authorising Officer with the original authorisation in the central record of authorisations managed by Legal and Democratic Services.

12.0 RECORDS AND ERRORS

12.1 Material obtained as a result of surveillance activities should be recorded on the "Record of Product obtained by Directed Surveillance Form".

12.2 A copy of this form should be forwarded to the Authorising Officer to be filed with the Authorisation form. The original should be retained by the Investigating Officer, as part of the case file. Internal procedures within some departments may require that all authorisations and case materials are held within a specified secure location.

12.3 A record must also be maintained of the period over which surveillance has taken place to assist with reviews and renewal applications.

12.4 There is a requirement set out in the OSC Procedures and Guidance 2014 to report all covert activity that was not properly authorised to the OSC in writing as soon as the error is recognised. This includes activity which should have been authorised but wasn't or which was conducted beyond the directions provided by the authorising officer. It is therefore important that when an error has been identified it is brought to the attention of the SRO in order to comply with this guidance. The Council has a responsibility to report to the Inspector at the commencement of an inspection all activity which should have been authorised but wasn't. This is to confirm that any direction provided by the Chief Surveillance Commissioner has been followed. This will also assist with the oversight provisions of the Councils' RIPA activity.

12.5 The reporting requirement does not apply to covert activity which is deliberately not authorised because an authorising officer considers that it does not meet the legislative criteria, but allows it to continue. This would be surveillance outside of RIPA.

13.0 HANDLING PRODUCTS FROM SURVEILLANCE ACTIVITIES

13.1 Product from Covert Surveillance activities may consist of: Photographs, Video film, Voice recordings, Surveillance log, Officers Notes

13.2 The above may be required as evidence in current or future criminal proceedings. Officers must have regard to the provisions of the Criminal Procedure and Investigations Act 1996 in relation to unused material. Product obtained via an authorisation may be used by the authority in other investigations.

13.3 Although specific legislation and the Data Protection Act 1998 provide for the disclosure of information in certain circumstances, additional controls are introduced by RIPA.

13.4 The use of any product obtained by authorised surveillance activities outside of the Public Authority or the Courts should only be authorised in the most exceptional circumstances. **Joint operations should make reference to the potential use of evidence by each agency.**

13.5 Officers may receive requests from other agencies for product, which may include photographs of suspects, descriptions, and vehicle details. Where this information has been obtained under an authorisation, further guidance should be sought from the Authorising Officer and if disseminated to an outside agency, meet the requirements of the Data Protection Act 1998.

14.0 STORAGE AND RETENTION OF PRODUCT

14.1 All material associated with an application, together with material obtained throughout a surveillance operation will be subject of the provisions of the Criminal Procedures Investigations Act 1996 (“CPIA”) Codes of Practice which state that relevant material in an investigation has to be recorded and retained and later disclosed to the prosecuting solicitor in certain circumstances. It is also likely that the material obtained as a result of a RIPA application will be classed as personal data for the purposes of the Data Protection Act 1998 (“DPA”).

14.2 Officers should make themselves aware of the provisions within the DPA and how it impacts on the whole RIPA process. Material obtained together with relevant associated paperwork should be held securely and any dissemination of the product must take account of the DPA and may only be disclosed to those that can lawfully receive it. The material may only be retained for as long as is necessary. Therefore material which will be retained outside of the CPIA provisions must have some justification to meet the DPA requirements. If in doubt advice should be sought from the RIPA Monitoring Officer.

14.3 Material which is required to be retained under CPIA should be retained until a decision is taken whether to institute proceedings against a person for an offence or if proceedings have been instituted, at least until the accused is acquitted or convicted or the prosecutor decides not to proceed with the case.

14.4 Where the accused is convicted, all material which may be relevant must be retained at least until the convicted person is released from custody, or six months from the date of conviction, in all other cases.

14.5 If the court imposes a custodial sentence and the convicted person is released from custody earlier than six months from the date of conviction, all material which may be relevant must be retained at least until six months from the date of conviction.

15.0 DISPOSAL OF PRODUCT

15.1 Officers should have regard to the fifth principle of the Data Protection Act 1998, as follows:

> Product, which is not required as evidence should not be retained any longer than necessary. It will be necessary to retain product for a sufficient period of time to safeguard Durham County Council against any civil claims against infringement of an individuals Human Rights. Refer to your service areas retention guidelines.

15.2 Product which has been destroyed should have this fact recorded on the record of product obtained by Directed Surveillance, and be signed by the Officer (See 10.0).

15.3 An amended copy of this Record form should be forwarded to the Authorising Officer, indicating destruction of the product obtained from the surveillance activity.

16.0 GUIDANCE NOTES FOR THE AUTHORISATION OF DIRECTED SURVEILLANCE

16.1 Does the activity involve:-

> The systematic covert surveillance of an individual (whether or not the identity is known), which is likely to gather personal information?

IF SO, AN AUTHORISATION IS REQUIRED

16.2 Low level activity for example, to determine whether a premise is still trading, will not require authorisation. Surveillance carried out in response to immediate events will also not require authorisation. However, if the surveillance activity continues for any period of time, an authorisation will be required.

16.3 **The Authorising Officer must be satisfied that:**

The authorisation is:

Necessary for the purposes of preventing or detecting criminal offences that are either punishable by at least a 6 month prison sentence or are related to the underage sale of alcohol or tobacco.

Consideration should also have been given to alternative methods of obtaining the evidence and why this has not or will not work or secure the best evidence.

16.4 **The Authorising Officer must also believe that the surveillance is proportionate to what it seeks to achieve, and is not excessive.**

Where the identity of the subject is known to the officer, measures should also be taken to verify, (where appropriate) the address under surveillance (e.g. electoral register, business rates, utility suppliers). The Authorising Officer may also wish to include some control measures within the authorisation e.g. reviews, circumstances in which the surveillance must be stopped.

16.5 The application should provide the background to the investigation, and details of other methods which have failed to provide the information being sought or why other methods are not appropriate.

16.6 The description of the activity to be undertaken should be as comprehensive as possible, describing how the surveillance will be undertaken, where it will occur and any equipment (e.g. cameras, video camera) which will be used. The Authorising Officer must know the capabilities of the equipment. The investigatory officers must not employ techniques which are not permitted by the authorisation.

16.7 The information being sought should be described and how this may provide evidence of the offence or other matter being investigated. The potential for collateral intrusion should be identified and plans to avoid / minimise such intrusion.

16.8 A statement must also be included as to the likelihood of obtaining confidential information as defined in the codes of practice.

16.9 If **confidential material**, is being sought, or **is likely** to be obtained, a higher level of authorisation is required. **This authorisation can only be given by the Chief Executive of Durham County Council, (or in his absence by a Chief Officer).** Further guidance should be sought if confidential material becomes relevant to the investigation.

16.10 Where applications for authorisation are refused by the Authorising Officer, records of the refused application must also be maintained stating the reasons for the refusal and a service number. Copies of these refusals must be sent for inclusion in the central record.

17. NECESSITY AND PROPORTIONALITY

17.1 Necessity

For interference with an individual's rights under 'Article 8' (Right to Privacy) to be necessary, the only ground on which the Council may authorise directed surveillance is for the prevention or detection of a criminal offence, punishable by a maximum term of at least 6 months imprisonment or are related to the underage sale of alcohol or tobacco. In order to be satisfied, the conduct that it is aimed to prevent or detect must be identified and clearly described. The

Authorising Officer must be satisfied that overt measures would not be likely to secure the desired result.

17.2 **Proportionality**

The proposed activity must be proportionate to what it seeks to achieve. The four elements of proportionality must be fully considered in an application.

1. Balance the size and scope of the operation against the gravity and extent of the perceived mischief.

2. Explain how and why the methods to be adopted will cause the least possible intrusion on the target and others.

3. Explain why the activity is an appropriate use of the legislation and the only reasonable way, having considered all others, of obtaining the necessary result; and

4. Provide evidence of other methods considered and why they were not implemented.

18. MEMBER OVERSIGHT

18.1 Elected members of a local authority should review the authority's use of RIPA and set the policy at least once a year. They should also consider internal reports on the use of RIPA on at least a quarterly basis to ensure that it is being used consistently with the Council's policy and that the policy remains fit for purpose. Members must not be involved in making decisions on specific authorisations. The Council's Corporate Issues Overview and Scrutiny Committee will carry out this function.

B. COVERT HUMAN INTELLIGENCE SOURCES (C.H.I.S.)

1.0 INTRODUCTION

1.1 This section of the guidance document, deals with Covert Human Intelligence Sources, more commonly known as: Undercover Officers, Informants/Agents

Authorisation is a two-stage process:

(a) to use a source
(b) an authority for the conduct of the source.

1.2 A Covert Human Intelligence Source is a person who establishes or maintains a personal or other relationship with another person for the covert purpose of:

(a) Using such a relationship to obtain information, or to provide access to information to another person, or

(b) Disclosing information obtained by the use of such a relationship or as a consequence of such a relationship.

1.3 The relationship is used covertly if, and only if, it is conducted in a manner calculated to ensure that the person is unaware of its purpose.

1.4 Durham County Council receives complaints routinely from the public and traders regarding the alleged activities of individuals. The actions of these complainants do not generally fall within the definition of a covert source, since they are a one off provision of information. However, a person may become a covert source if an ongoing relationship with a public authority (Durham County Council) develops and activities described in paragraph 1.2 above are carried out.

1.5 Where the nature of the complaint relates to a matter where an officer requests the complainant to obtain further information covertly, via a relationship with another individual, this activity is likely to fall within the scope of the Act. An authorisation will therefore be required before seeking such information. By following the authorisation procedures, the Authority will also be in a position to seek to safeguard the identity of the source in any subsequent legal proceedings. The origin of any information from the source can be withheld, subject to acceptance by the court of the established **Public Interest Immunity,** disclosure procedures. Further guidance should be sought from Legal Services on this issue, to ensure that the identities of any such individuals are safeguarded in the event of any legal proceedings, tribunals or disciplinary hearings.

1.6 The Code of Practice on Covert Human Intelligence Sources relates not only to sources (which may commonly be referred to as informants) but also the activities of sources, which consist of undercover officers who establish or maintain a covert relationship to obtain information and evidence.

1.7 Before a source may be engaged or an undercover officer deployed the **use and conduct** must be authorised. The use part of the authorisation, effectively registers the source with the Authority. The conduct part addresses what the source is tasked to do. The applicant must not be the source.

1.8 In most cases, the use and conduct of a source will be restricted to a single investigation. However, situations may arise, where different conducts are required as the investigation develops. Consideration should then be given to cancelling the original authorisation and seeking a new authorisation on the basis of the new circumstances of the investigation.

1.9 The same authorisation form is used for both use and conduct. A handler and controller must also be designated, as part of the authorisation process, and detailed records of the use, conduct and tasking of the source maintained.

1.10 An Authorising Officer is a person entitled to give an authorisation for the use or conduct of a source in accordance with Section 29 of the Regulation of Investigatory Powers Act 2000. A list of the Authorising Officers is held in the **central record** managed by the RIPA Monitoring Officer, on behalf of the SRO. All Authorising Officers are, however, corporate and therefore can cross service authorise.

1.11 The use of Covert Human Intelligence sources should be necessary and proportionate to the matter being investigated.

1.12 Failure to obtain an authorisation may render Durham County Council liable to a claim of infringing the human rights of an individual and may adversely affect the admissibility of any evidence obtained by the use of covert methods employed by a source. It is also established that a Public Authority owes a duty of care to a CHIS. Failure to undertake a robust risk assessment and authorisation may also adversely affect the position of the Authority in the source suffering any harm as a result of the activity in which they have been engaged.

1.13 Careful consideration must be given to any potential sensitivities, which may exist, before deciding whether to use a CHIS in a particular community or against a particular individual.

1.14 A separate **directed surveillance** authorisation is **not** required where any surveillance device (technical equipment) is used in the presence of the covert source.

1.15 A Covert Human Intelligence source carrying surveillance equipment **can** be invited to enter residential premises or a private vehicle. However the CHIS **cannot install** surveillance equipment in residential premises since this activity constitutes intrusive surveillance or a private vehicle, since this activity constitutes property interference. These techniques are not available for use by Local Authorities.

2.0 GUIDANCE ON THE SOURCE CULTIVATION PROCESS

2.1 When seeking an authorisation for an individual to act as a covert human intelligence source, consideration needs to be made of their potential role in the investigation. Are they prepared to be a witness? Do they need to be given protection as a result of providing information, by means of public interest immunity? The source may also be in a position to provide information relating to a number of different matters worthy of investigation.

2.2 The motives of potential sources need to be considered as part of the evaluation process. Could they be motivated by possible rewards or revenge? The aim could be to deflect attention away from themselves towards other individuals.

2.3 Has consideration been given to building up a detailed profile of the potential source and their associates. **In all cases**, a face-to-face meeting with the complainant or any other person considered as a potential source should take place. Please be aware that the individual may have needs in respect of language, hearing or sight.

2.4 Directed surveillance may be needed to evaluate the source. Consideration should be given in certain circumstances to carrying out checks on the source with the Police. A thorough risk assessment must be carried out on the potential source, and the proposed conduct.

3.0 MANAGEMENT OF SOURCES

3.1 Tasking is the assignment given to the source by the handler/controller asking him/her to obtain information or to take action to obtain information.

3.2 All authorisations **should be in writing** and in place before tasking a source. Every source must have a designated handler and controller.

4.0 DESIGNATED HANDLERS AND CONTROLLERS FOR THE USE OF COVERT HUMAN INTELLIGENCE SOURCES

4.1 Where the Covert Human Intelligence source is a complainant or an informant, the Handler will be the Investigating Officer and the Controller will be their line manager. Where the Covert Human Intelligence source is an Officer of the authority acting in an undercover capacity the Handler will be the Officer's line manager and the Controller will be another manager within the Service. This arrangement will ensure that an Officer does not act as a Controller and Authorising Officer thereby ensuring a level of independent scrutiny.

5.0 SECURITY AND WELFARE OF SOURCES

5.1 A source has no licence to commit crime. In certain circumstances it may be advisable to provide written guidance to the source, explaining what is being requested of them and the limits of the tasking. The source should be asked to sign such a document to confirm that they understand the terms of reference.

5.2 A public authority deploying a source, should take into account the safety and welfare of the source, when carrying out any actions in relation to the authorisation or tasking. The foreseeable consequences of the tasking should also be considered.

5.3 A Risk Assessment should be undertaken to evaluate the source and to determine the risk to the source of any tasking and the likely consequences should the identity and role of the source become known to the subject or others involved with the subject. Appropriate documentation is contained on the intranet or is available from the RIPA Monitoring Officer.

5.4 The handler should draw to the attention of the controller:

The Risk Assessment
The Conduct of the Source
The Safety and Welfare of the Source.

A Handler is responsible for:

Dealing with the source on behalf of the Authority
Directing the day to day activities of the source
Recording the information supplied by the source
Monitoring the security and welfare of the source.

5.5 Where a source is known or suspected of being involved in crime, consideration should be given to their motives in supplying information. It may also be a prudent step in the management of such a source to have two officers present during any meetings with the source. Background checks on the potential source via the Police Local Intelligence Officer should also be considered.

5.6 Special provisions exist for the conduct in use of juvenile sources (Under 18).

A source under 16 cannot be engaged to use a relationship with any person having parental responsibility for them. A source under 16 must have an appropriate adult present during any meetings and a risk assessment must also take place before granting or renewing an authorisation for the conduct and use of a source under 16. This will take account of physical and psychological risks.

See the Regulation of Investigatory Powers (Juveniles) Order 2000 for detailed guidance.

5.7 Special consideration should also be given to the use of vulnerable individuals as a source. This will require the highest level of authorising officer, the Chief Executive (see the code of practice for further guidance).

5.8 Authorisations for juvenile sources i.e. a source under the age of 18, when the authorisation is granted have effect for **one month**. **Juvenile source** authorisations should be issued by the highest level of authorising officer in an Authority. This will be the **Chief Executive** of Durham County Council.

6.0 JUDICIAL APPROVAL OF CHIS APPLICATIONS

6.1 From 1 November 2012 a local authority who wishes to authorise the use of a CHIS will need to obtain an order approving the grant or renewal of an authorisation or notice from a Justice of the Peace (a District Judge or Lay Magistrate) before it can take effect. If the Justice of the peace is satisfied that the statutory tests have been met and that the use of a CHIS is necessary and proportionate, he/she will issue an order approving the grant or renewal for the use of the technique as described in the application.

7.0 DURATION OF AUTHORISATIONS

7.1 Authorisations have effect for a period of twelve months from the date of judicial approval unless a juvenile in which case the authorisation has effect for a period of one month. The Authorisation should be managed and be made subject to reviews set as a control measure by the Authorising Officer.

7.2 Records of authorisations are to be retained for, a minimum period of one year to comply with the code. However, it will be policy to retain the records for a **period of six years,** to safeguard against any civil claims against the authority under the Human Rights Act 1998.

7.3 Destruction of the authorisation form should be documented in the Authorising Officers Management Record file.

8.0 RENEWALS AND REVIEWS

8.1 An authorisation may be renewed, after the Authorising Officer reviews the use made of the source having regard to:-

a) The tasks given to the source
b) The information obtained from the source.

If satisfied that the original authorisation criteria are met, a renewal may be authorised. A renewal of a grant of a CHIS authorisation must be approved by a Justice of the Peace before it can take place.

8.2 Since an authorisation for a CHIS may remain in force for a period of twelve months, regular reviews should be undertaken to ensure the ongoing validity of the activity and the ongoing welfare and security of the source. Any changes to circumstances may require that further risk assessments are undertaken.

8.3 The reviews should be undertaken at intervals of **no longer than three months** and documented. Additional **control measures** may also be introduced as a result of a review. The Authorising Officer should implement a system to identify appropriate review dates (e.g. the MS Exchange Calendar alarm option).

9.0 CANCELLATIONS

9.1 An Authorising Officer must cancel an authorisation where:

The use or conduct of the source no longer meets the original authorisation criteria.

The procedures for managing the source are no longer in place.

Where possible the source should be informed of the cancellation, and this fact noted on the cancellation.

9.2 Where an investigation no longer requires the authorisation to be in place e.g. the evidence has been obtained, it should be cancelled promptly rather than allowed to expire through time, and the reason for cancellation documented.

10.0 SOURCE RECORDS

10.1 Records of Use of the source and the product provided by the source. Similarly for the procedures detailed for Directed Surveillance records should be maintained by the service, for a **period of six years**. Records should not be destroyed without the authority of the Authorising Officer. Destruction of records should be documented in the Authorising Officers Management Records file.

10.2 The following information must be recorded:-

- Authorisation Reference Number
- Authorising Officer
- Identity used by Source (If any)
- Identity of Source

- Reference used in the authority to refer to Source (If any)

- Information relating to security and welfare of Source

- A record that any risks to the security and welfare of the Source have been explained to and understood by the Source

- Records of reviews conducted on the continuing use and welfare of the Source

- The date when the Source was recruited

- The circumstances of the recruitment

- Identity of the Handler and Controller (and details of any changes)

- A record of the tasks and activities given to the Source

- A record of all contacts or communications between the Source and a person representing the Authority

- The information obtained through the Source

- How the information is used

- A statement as to whether any payment, benefit or reward is provided by or on behalf of any investigating authority and details of it **(#)**

- Reasons for cancelling / not renewing the authorisation and the date and the time of such a decision.

(it is **NOT** currently the Policy of Durham County Council to directly offer any benefits or rewards to a CHIS. Rewards may be forthcoming from a third party e.g. from a trade association or trademark holder where an investigation involves counterfeit goods).

11.0 THE APPLICATION FOR AUTHORISATION

Must include:

11.1 The grounds on which the authorisation is sought: and why it is necessary

Preventing or detecting crime or preventing disorder

- An explanation of the ***proportionality*** of the Use/Conduct.

- Where the matter relates to a specific investigation, details of that investigation or operation.

- Details of the purpose for which the source will be tasked.

- Details of what the source will be tasked to do.

- Details of the level of authority required having regard to any confidential material that might be obtained as a consequence of the authorisation. (This will invoke the requirement to be authorised by the Chief Executive if confidential material is being sought or is likely to be obtained).

- Details of who will be affected, and plans to avoid/minimise collateral intrusion. Where this changes, the Authorising Officer must be informed and the authorisation reviewed.

- A detailed Risk Assessment must have been undertaken. A review may also be required if the assessment is not current.

- The Authorising Officer may wish to impose ***control measures*** on the authorisation that is granted.

11.2 Unless renewed or cancelled, an authorisation remains in force for:

12 months from the date of judicial approval (Juveniles One Month). The authorisation should be given a unique operation reference number and be recorded in management record file. Conduct authorisations should be referenced to the original use authorisation.

A duplicate/copy of the authorisation should be issued to the officer. This will ensure that the officer has a record of the scope of the activity authorised.

11.3 Applications, which are refused, should also be recorded together with the reasons for the refusal and a service number. Copies of these refusals must be sent for inclusion in the central record.

12.0 ERRORS

12.1 There is now a requirement as set out in the OSC procedures and Guidance 2011 to report all covert activity that was not properly authorised to the OSC in writing as soon as the error is recognised. This includes activity which should have been authorised but wasn't or which was conducted beyond the directions provided by the authorising officer. It is therefore important that when an error has been identified it is brought to the attention of the SRO in order to comply with this guidance. The Council has a responsibility to report to the Inspector at the commencement of an inspection all activity which should have been authorised but wasn't. This is to confirm that any direction provided by the Chief Surveillance Commissioner has been followed. This will also assist with the oversight provisions of the Councils' RIPA activity.

12.2 This does not apply to covert activity which is deliberately not authorised because an authorising officer considers that it does not meet the legislative criteria, but allows it to continue. This would be surveillance outside of RIPA.

C. RISK ASSESSMENTS

1. Whenever undertaking covert directed surveillance, or engaging in the conduct and use of a Covert Human Intelligence Source, the proposed activity **must** be the subject of a suitable and sufficient risk assessment and evaluation of the proposed Source.

2. Directed Surveillance activities clearly have the potential to expose staff to hazards, should their activities become known to the subject or even to others during the operation. The use of Covert Human Intelligence Sources has the potential to expose handlers, undercover officers, agents/informants and the public to health and safety risks. A duty of care may also lie with officers and the Authority in managing sources.

3. Authorising Officers, Controllers, Handlers Undercover Officers and Investigating Officers **must** all have regard to Durham County Council Corporate Policy on Health and Safety. This addresses issues such as lone working and violence to staff.

4. The Policy states that "Durham County Council will ensure that management systems are produced that are sufficient to effectively identify, assess, manage and control the risks to the health and safety of employees and other people affected by their work".

5. It is a matter for each Service to determine the training required to ensure that staff are competent to undertake risk assessments of proposed operations/use of covert sources. All incidents/dangerous occurrences during the course of operations should be reported in accordance with the corporate Health and Safety Procedures.

6. Consideration should also be given to staff training requirements to engage in covert activities, surveillance and acting in an undercover capacity.

7. This section of this guidance document is intended to provide an overview, which must be borne in mind when undertaking activities within the scope of RIPA.

8. Further Guidance on Health and Safety issues is available from:

   Management of Health and Safety at Work Regulations1999

   The Corporate Health and Safety Policy Document and Guidance

   The Health and Safety Unit (0191 383 3430)

9. Risk assessments for directed surveillance operations, should be undertaken by the officer in charge of the proposed activity and submitted with the authorisation application.

10. Risk assessments for the use of a CHIS, should be undertaken by the Handler and considered by the Controller as part of a risk management process. The assessment should then be forwarded to the Authorising Officer with the application. The assessment should consider the **Ethical, Personal** and **Operational Risks** of the proposed activity. The evaluation of a potential source is an important part of the application process.

11. Risk assessment is not a one off activity, but an ongoing process throughout the operation and use of the source, since circumstances may change and a review may be required.

12. The nature of the risks surrounding the deployment and management of individual sources, handlers and operational activities will vary according to a wide range of factors on a case by case basis. Risk assessment allows the handler and controller to advise the Authorising Officer of the plan for managing the risks.

13. Authorising Officers will **not** authorise a Directed Surveillance operation or the use of a source, without the evidence that the risks have been considered and a plan for their management exists.

D. RECORDING OF TELEPHONE CONVERSATIONS

1. **The interception of communications sent by post or public telecommunications systems or private telecommunications systems attached to the public network may only be authorised by the Secretary of State. (Part I Regulation of Investigatory Powers Act 2000).**

2. The attachment of a surveillance device to a telecommunications system can only be undertaken under a warrant issued under Section 5 of the Act (this is not available to the County Council).

3. An exception to the rule requiring a warrant exists, where one party to the conversation consents and where an authorisation for **directed surveillance** is obtained. See Section 48(4) of the Act.

4. For example, a member of the public may consent to the recording of a telephone conversation made by or to him/her. An officer may seek to record such a conversation to assist with an investigation into another person's activities.

5. An officer may also request a colleague to telephone another person as part of an investigation, or may make the call himself or herself. These situations may require an authorisation to be granted if the RIPA criteria are met.

6. Officers considering making a test purchase must be very careful when deciding whether the recorded conversation, is to obtain goods, or whether it is to gather information, which will only be obtained in a covert capacity.

E. ACCESSING COMMUNICATIONS DATA

1.0 Introduction

1.1 This section of the guidance document details the system in place to ensure compliance with RIPA, when an investigating officer seeks to obtain communications data within the scope of their enquiries.

1.2 In a similar manner to the existing provisions of RIPA relating to directed surveillance and the use of Covert Human Intelligence sources, a process of submitting an application and securing an authorisation is established by the legislation and code of practice.

1.3 The Council processes its RIPA applications for communications data via the the National Anti Fraud Network (NAFN). NAFN operates a secure online system for the acquisition of communications date under RIPA. NAFN officers act as Single Points of Contact or SPoC's to ensure that Council applications meet the necessary standards before the application is approved by a Designated Person (DP) who is an officer within the Council. Whilst the NAFN system makes it easier to comply with the law, the SRO retains oversight of the process to ensure that it is carried out in a lawful manner and in accordance with the statutory code of practice.

Further guidance on NAFN can be obtained from the RIPA Monitoring Officer.

1.4 From 1 November 2012 a local authority who wishes to authorise the use to acquisition of communications data, will need to obtain an order approving the grant or renewal of an authorisation or notice from a Justice of the Peace (a District Judge or Lay Magistrate) before it can take effect. If the Justice of the Peace is satisfied that the statutory tests have been met and that the use of the acquisition of communications data, is necessary and proportionate, he/she will issue an order approving the grant or renewal for the use of the technique as described in the application.

1.5 If an application is to be approved by a Justice of the Peace, an accredited individual within NAFN forwards a notice to the communications service provider (CSP), to obtain the information. This activity cannot be undertaken by an officer, as CSPs will only accept requests for information from accredited officers registered with the Home Office and termed Single Points of Contact (SPOC).

1.6 Records of all applications, authorisations, notices, cancellations and refusals must be maintained since an inspection regime by the Interception of Communications Commissioner's Office is established under this part of the legislation, making Council procedures and documentation subject to periodic inspection by an external body. These records are held by NAFN but authorisations approved by a Justice of the Peace are retained by the Council in a central record in a similar manner to directed surveillance and CHIS authorisations.

2.0 WHAT IS COMMUNICATIONS DATA

2.1 NAFN are able to obtain communications data from specific telecommunication sources i.e. telephone, e-mail, web address and postal providers. Information obtainable under RIPA is formed into the following three distinct types:

(A) Data
This is not available to Local Authorities.
Classed as “traffic data” comprised in or attached to a communication.
e.g. information identifying the sender and recipient, mobile phone cell site location, pages visited on a website, I.P Address, information on the outside of a parcel, incoming call data.

(B) Data
Classed as any information regarding the use of a service made by any person that does not include contents.
- Itemised outgoing call records only
- Timings and durations of calls
- Call forwarding

(C) Data
Classed as any information held by a telecommunication company not defined as (A) Data or (B) Data,
- Subscriber details
- Payment details
- Top up history
- Connection dates
- Account history
- Royal mail - redirection, PO Box, freepost, registered and franked details
- Website provider

3.0 RECORDS AND ERRORS

3.1 A copy of each authorisation will be maintained by the DP and supplied to the central record of authorisations managed by Legal and Democratic Services.

3.2 Where any errors have occurred in granting authorisations or notices (e.g. subscriber details of an incorrect telephone number being obtained), or more data has been supplied by the CSP than that requested, i.e. obtaining excess data, a record must be kept and the matter reported to the Interception of Communication Commissioner’s Office as soon as practicable. A copy of the error record must also be provided to NAFN and to the RIPA Monitoring Officer.

F. SOCIAL NETWORKING SITES AND INTERNET SITES

1. Although social networking and internet sites are easily accessible, if they are going to be used during the course of an investigation, consideration must be given about whether a RIPA authorisation should be obtained.

2. Whilst it is the responsibility of an individual to set privacy settings to protect against unsolicited access to their private information on a social networking site, and even though the data may be deemed published and no longer under the control of the author, it is unwise to regard it as "open source" or publicly available; the author has a reasonable expectation of privacy if access controls are applied. Where privacy settings are available but not applied the data may be considered open source and an authorisation is not usually required. The frequent or systematic check on an open source record could amount to directed surveillance and the appropriate authorisation would be needed.

3. If it is necessary and proportionate for the Council to covertly breach access controls, the minimum requirement is an authorisation for directed surveillance. For example, an authorisation for directed surveillance will be required if an investigating officer is planning to monitor open source information on an individual's social networking site (i.e. the activity is more than a one off search for information). An authorisation for the use and conduct of a CHIS is necessary if a relationship is established or maintained by the officer (i.e. the activity is more than mere reading of the site's content). This could occur if an officer covertly asks to become a "friend" of someone on a social networking site. The officer seeking the authorisation should fully consider the issue of collateral intrusion (See Part A, Section 2.0).

4. A CHIS authorisation is unlikely to be required when using an internet trading organisation such as E-bay or Amazon Marketplace. The use of a disguised purchaser details in a simple, overt, electronic purchase does not usually require a CHIS authorisation, because no relationship is usually established at this stage. A CHIS authorisation is required in circumstances when a covert relationship is likely to be formed, for example when liaising via Facebook or other types of site which do not allow for more traditional transactions and where the investigating officer has to make contact with the seller directly and would wish for their true identity or reason for purchasing to be unknown to the seller.

5. The Council's Environment Health and Consumer Protection Service has developed an Online Investigation Protocol which should be adopted by other service areas conducting online investigations.

G. JOINT AGENCY SURVEILLANCE

1. In cases where one agency is acting on behalf of another, it is usually for the tasking agency to obtain or provide the authorisation. For example, where surveillance is carried out by Council employees on behalf of the Police, authorisation would be sought by the Police. If it is a joint operation involving both agencies the lead agency should seek authorisation.

2. Council staff involved with joint agency surveillance are to ensure that all parties taking part are authorised on the authorisation page of the application form to carry out the activity. When staff are operating on another organisation's authorisation they are to ensure they see what activity they are authorised to carry out and make a written record. They should also provide a copy of the authorisation to the RIPA Monitoring Officer. This will assist with oversight of the use of Council staff carrying out these types of operations.

H. NON-RIPA SURVEILLANCE

1. Amendments to the Regulation of Investigatory Powers (Directed Surveillance and Covert Human Intelligence Sources) Order 2010 mean that a local authority can now only grant an authorisation under RIPA where the local authority is investigating criminal offences which attract a maximum custodial sentence of at least six months or criminal offences relating to the underage sale of alcohol or tobacco.

2. As a result of the changes in legislation, it is envisaged that surveillance may be required which falls outside of RIPA (for example in the case of anti-social behaviour offences which do not attract a maximum custodial sentence of at least six months imprisonment). The Office of Surveillance Commissioners Procedures and Guidance 2011 states that it is prudent to maintain an auditable record of decisions and actions to use covert surveillance without the protection of RIPA and that such activity should be regularly reviewed by the SRO. The SRO will therefore maintain an oversight of non RIPA surveillance in her role as SRO to ensure that such use is compliant with Human Rights legislation. The RIPA Monitoring Officer will maintain a central record of non RIPA surveillance.

3. As part of the new process of formally recording and monitoring non RIPA surveillance, a non RIPA surveillance application form should be completed and authorised by at least a tier 4 level manager. A copy of the non RIPA surveillance application form can be found on the Intranet or is available from the RIPA Monitoring Officer.

4. Non RIPA surveillance also includes staff surveillance which falls outside of RIPA. Any surveillance of staff must be formally recorded on the non-RIPA surveillance Application Form and authorised by the Head of Service in consultation with the Head of Internal Audit. A central record of staff surveillance is also maintained by the SRO.

I. AUDITING OF AUTHORISATIONS AND RECORDS

1. Periodic audits will be carried out across relevant services, including the Central Record. These will be conducted by internal Audit in line with the Council's Risk Based Strategic Audit Plan. This may require some material to be sanitised, to maintain the safety of sources.

2. The following should fall within the scope of the audit:

   Applications
   Authorisations
   Risk Assessments
   Reviews and Renewals
   Cancellations
   Records of Product of Directed Surveillance
   Source Records
   Staff Awareness e.g. training, memos, e-mails, meetings
   Access and awareness of the codes of practice.

3. The audit should seek to establish compliance of the authorisations/ renewals/reviews/cancellations and records, with RIPA and the Codes of Practice, and Durham County Council's, RIPA 2000 Guidance Document

J. COMPLAINTS

1. Copies of the Codes of Practice on Covert Surveillance and Property Interference and Covert Human Intelligence Sources are available to the public at Durham County Council, County Hall Help Desk. Copies should also be available at public offices of Durham Council departments undertaking activities, which are within the scope of RIPA.

2. The Investigatory Powers Tribunal (IPT) exists to investigate complaints about conduct by various public bodies under RIPA.

   The Tribunal can be contacted at:

   The IPT
   PO Box 33220
   London
   SW1H 97Q

   Tel: 0207 035 3711
   www.ipt-uk.com

K. MANAGEMENT RECORDS

1. The Authorising Officer must keep a copy of the relevant documents to check against the cancellation. These documents must be kept in a secure place, with restricted access. **Original authorisations (including refusals), reviews, renewals and cancellations, must be provided to the Central Record for Durham County Council.** This is managed by the RIPA Monitoring Officer in Legal and Democratic Services. Officers forwarding confidential material to the Central Record must ensure that it is forwarded by a secure method.

2. The Central Record is held in a locked filing cabinet.

   The following officers have sole access to the central record:

   The Director of Corporate Resources

   Head of Legal and Democratic Services (SRO)

   Legal Manager - Governance

   RIPA Monitoring Officer

3. **The Record Retention Period is 5 years**

APPENDIX 1

RIPA DIRECTED SURVEILLANCE/CHIS AUTHORISING OFFICERS

Authorising Officer	Rank
Paul Bradley	Chief Internal Auditor and Corporate Fraud Manager Resources
Ian Hoult	Neighbourhood Protection Manager Adults and Health Services
Owen Cleugh	Consumer Protection Manager, Adults and Health Services

RIPA COMMUNICATIONS DATA DESIGNATED PERSONS

Designated Person	Rank
Owen Cleugh	Consumer Protection Manager, Adults and Health Services

APPENDIX 2

DURHAM COUNTY COUNCIL

REGULATION OF INVESTIGATORY POWERS ACT 2000

CCTV SYSTEM PROTOCOL

1.0 Introduction

1.1 Durham County Council operates and manages a number of Surveillance Cameras and Closed Circuit Television Systems (CCTV) for the purposes of monitoring public open space to deter anti-social behaviour, preventing and detecting crime and to monitor council buildings, vehicles and premises for security reasons.

1.2 It is recognised that CCTV systems may be employed to observe and record the activities of individuals, which clearly has implications under the Human Rights Act 1988 and the Regulation of Investigatory Powers Act 2000, (RIPA) in terms of intrusion into the privacy of individuals.

1.3 This protocol is a separate document to the Council's CCTV Policy and Code of Practice produced by Durham County Council in response to the code of practice issued by the Information Commissioner to ensure compliance with the Data Protection Act 1998. Officers seeking to make use of CCTV systems and recordings should, however, have regard to the requirements of the Council's policy.

1.4 This protocol serves to establish safeguards for the potential use of CCTV systems to specifically target individuals to observe and/or record their activities. Such planned activities will fall within the scope of Directed Surveillance and are subject to the controls established by RIPA to ensure that the activity is necessary, proportionate and authorised by a suitable senior officer of the authority.

1.5 Durham County Council is committed to promoting a just society that gives everyone an equal chance to live, work and live free from discrimination and prejudice. This protocol, demonstrates our concern for human rights, and therefore contributes to our diversity agenda.

2.0 Authorised Activities

2.1 General, non-directed recording of events and people, through the use of overt CCTV systems, will not infringe the rights of the individual. This activity does not, therefore, need to be authorised, through the RIPA process.

2.2 The retrospective viewing of CCTV footage, to gain evidence of actual or potential criminal activity, does not fall within the definition of covert surveillance and would, similarly, not require any form of authorisation. An approach should be made to the County Hall Facilities Manager, for permission to view. Similarly for sites other than

County Hall, the officer in charge of the premises should be approached in the first instance.

2.3 The processing of such data is, however, subject to the Information Commissioner's Code, issued under the Data Protection Act 1998.

2.4 Provision also exists within the RIPA framework, to react to immediate events, without the need to obtain an authorisation. For example, should a CCTV operative witness an attempted break-in of any property, it would be completely in order to re-focus or target the camera on that particular activity.

2.5 However, on occasions, it can be useful to use this equipment to detect or prevent crime, by means of a planned operation to record the activities of known or unknown persons. A comprehensive, corporate guidance document exists, to clearly define the processes and procedures that must be followed if such use is to be contemplated.

2.6 In these instances, CCTV operatives must not carry out targeted, planned surveillance which falls within RIPA, without an appropriate authorisation.

2.7 It is not the responsibility of the CCTV operative to obtain such authorisation, which must **always** be in existence **prior** to any such activity commencing. Any individual approaching a CCTV operative without such an authorisation, should be referred to the Senior Responsible Officer and be advised that any unauthorised use of the CCTV system would be unlawful and may give rise to a claim against the authority.

2.8 On occasions, the authority may be approached by an outside law enforcement agency to help in their enquiry, by utilising the authorities CCTV equipment, to undertake planned covert surveillance. Any approach of this nature, must be referred to the Senior Responsible Officer and no such usage should ever be approved unless the agency concerned produces a valid RIPA authorisation.

This document can be provided in different formats and languages on request. Please call Laura Ackermann on 03000 269326