**REGULATION OF INVESTIGATORY POWERS ACT 2000**
**POLICY DOCUMENT**
**NOVEMBER 2012**

## INTRODUCTION

In some circumstances it may be necessary for Derbyshire County Council employees, in the course of their duties, to make observations of a person or persons in a covert manner, i.e. without that person's knowledge. By their nature, actions of this sort may constitute an interference with that person's right to privacy and may give rise to legal challenge as a potential breach of Article 8 of the European Convention on Human Rights and the Human Rights Act 1998 – the right to respect for private and family life.

On the 25 September 2000 the Regulation of Investigatory Powers Act 2000 was brought into force in England and Wales. The purpose of the Act was to ensure that all public authorities were able to carry out covert surveillance on a statutory basis without breaching the Human Rights Act 1998. The provisions of this Act have subsequently been modified in respect of public authorities by the provisions of the Protection of Freedoms Act 2012 – Changes to Provisions Under the Regulation of Investigatory Powers Act 2000 (RIPA) which requires that, from 1st November 2012, local authorities wishing to use the provisions of RIPA require any authorisations or notices to be subject to a separate authorisation by a Justice of the Peace. Also a local authority can now only grant an authorisation under RIPA for the use of directed surveillance where the local authority is investigating criminal offences which attract a maximum custodial sentence of six months or more or criminal offences relating to the underage sale of alcohol or tobacco.

Covert surveillance enables public bodies to detect and/or prevent a crime that has been or is about to be committed and also to obtain information about an individual's or organisation's activities for these purposes.

Derbyshire County Council is committed to complying with the Act to ensure that an investigation is carried out properly and that the investigation is necessary and proportionate to the alleged offence. Obtaining information to assist an investigation may involve use of a human intelligence source; an investigation may also involve the acquisition of communications data.

The purpose of this Policy is to ensure that the proper procedures are in place in order to carry out covert surveillance; to ensure an individual's right to privacy is not breached; that proper authorisation is obtained for covert surveillance; that the proper procedures have been followed; that covert surveillance is considered as a last resort having exhausted all other avenues.

Derbyshire County Council's Policy is therefore implemented and followed in accordance with the Regulation of Investigatory Powers Act 2000.

## DEFINITIONS

### Authorising Officer (AO)

An Authorising Officer is an employee of Derbyshire County Council who has received adequate training and has attained a level of competency to be able to provide authorisation. Applications for surveillance will be authorised at the level of Director, Head of Service, Service Manager or equivalent as prescribed in the Regulation of Investigatory Powers (Directed Surveillance and Covert Human Intelligence Sources) Order 2010.

### CHIS

CHIS is defined as a Covert Human Intelligence Source and procedures for the authorisation of a CHIS are set out under Section 29 of RIPA 2000. A CHIS is a person who is required to establish or maintain a personal or other relationship with someone to obtain information in order to assist an investigation. Other relationships can include professional, business or working relationships. A CHIS is therefore the person who acts covertly and passes information to the designated handler.

### Collateral Intrusion

Collateral Intrusion is where the surveillance indirectly intrudes into the privacy of individuals who are not the direct subject of the surveillance eg where innocent bystanders are observed in the course of a covert surveillance operation – children are included within this definition. The application for authorisation should include an assessment of the risk of Collateral Intrusion and the Authorising Officer should consider this when assessing proportionality.

### Communications Data

Communications Data is data generated, held or obtained in the provision, delivery and maintenance of communications services, those being postal services or telecommunications services. It does not include the contents of the communication itself.

### Confidential Information

Confidential personal information is information held in confidence relating to the physical or mental health or spiritual counselling concerning an individual. Confidential journalistic information includes information acquired or created for the purposes of journalism and held subject to an undertaking to hold it in confidence. Confidential Information also consists of matters subject to legal privilege – the provision of professional legal advice to a client and including both oral and written communications. The Regulation Of Investigatory Powers (Covert Surveillance and Property Interference : Code of Practice) Order 2010 extends the definition of confidential information to include

constituent's communications with MPs on constituency business. Where it is likely that confidential information will be acquired only the Head of Paid Service (Chief Executive) or in his absence a designated Chief Officer may authorise the use of surveillance.

**Designated Handler**

A Designated Handler is responsible for directing the day to day activities of the CHIS as well as the security and welfare of the CHIS.

**Human Rights Act**

The Human Rights Act 1998 Section 6 provides protection to an individual's right to privacy.

**Intrusive Surveillance**

Intrusive Surveillance is available only to the Police or other law enforcement agencies. Intrusive surveillance is surveillance undertaken covertly which is carried out in relation to anything taking place on residential premises without the person's consent or in any private vehicle and must involve the presence of an individual on the premises or in the vehicle and may be carried out by the means of a surveillance device. Local authorities are not authorised to undertake intrusive surveillance.

**Investigating Officer (IO)**

An Investigating Officer is an officer within the Council who is involved in undertaking a specific investigation or operation.

**Necessity**

Necessity requires that covert surveillance take place when there are no reasonable and effective alternative (overt) means of achieving the desired objective.

**Private Information**

Private Information includes any information relating to a person's private or family life. This includes the right to establish and develop relationships with other human beings and activities that are of a business or professional nature.

**Private Vehicles**

Private Vehicles are subject to RIPA 2000 where any vehicle is used primarily for the private purposes of the person who owns or for a person otherwise having the right to use it.

**Proportionality**

If the activities are necessary then the Authorising Officer must believe that the activity is proportionate to the likely outcome. The activity will not be proportionate if it is considered excessive in the circumstances of the case, or if the information could have reasonably been sought by other less intrusive means bearing in mind any collateral intrusion caused.

**Public Authority**

Public Authority means any public authority within the meaning of Section 6 of the Human Rights Act 1998. Courts and tribunals are public authorities.

**Residential Premises**

Residential premises are subject to RIPA 2000 where premises are being occupied or used by any person, however temporarily, for residential purposes or otherwise as living accommodation (including hotel or prison accommodation that is so occupied or used). Residential Premises does not include common parts of blocks of flats.

**RIPA 2000**

RIPA 2000 stands for the Regulation of Investigatory Powers Act 2000.

**Surveillance**

Includes monitoring, observing or listening to persons, their movements, conversations or other activities and communications. It may be conducted with or without the assistance of a surveillance device and includes the recording of any information obtained.

**Covert Surveillance**

Covert Surveillance means surveillance that is carried out in a manner calculated to ensure that the person subject to the surveillance is unaware that it is taking place. Where covert surveillance activities are unlikely to result in obtaining private information about a person, or where there is a separate legal basis for such activities, neither the 2000 Act nor the revised Code need apply. However the actions of the Authority must still comply with the requirements of the Human Rights Act where there may be an Article 8 privacy intrusion.

**Directed Surveillance**

Directed Surveillance is defined in Section 26 (2) of RIPA 2000 as being surveillance which is covert but not intrusive and is undertaken for the purposes of a specific investigation or operation; in such a manner as is likely to result in the obtaining of private information about a person (whether or not one specifically identified for the purposes of the investigation or operation);

and 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 practical for an authorization under Part II of the 2000 Act to be sought for the carrying out of the surveillance. Thus, the planned covert surveillance of a specific person, where not intrusive, would constitute directed surveillance if such surveillance is likely to result in the obtaining of private information about that, or any other person.

**Surveillance Device**

Surveillance Device means any apparatus designed or adapted for use in surveillance.

## UNDERTAKING COVERT SURVEILLANCE

Under Part II of the Regulation of Investigatory Powers Act 2000 public authorities are authorised to undertake covert surveillance which is either directed surveillance or the use of a Covert Human Intelligence Source (CHIS). The authorisation must be necessary for the purpose of preventing or detecting crime or of preventing disorder.

Directed surveillance is defined under Section 26(2) of RIPA 2000 as being covert, must not be intrusive and is undertaken for the following purposes:-

- as a specific investigation or specific operation,

- to obtain private information about a person,

- otherwise than as an immediate response to events, in circumstances where it would not have been reasonably practical for an authorisation to be obtained.

Covert human intelligence source is defined under Section 26(8)(a-c) of RIPA 2000 where information is obtained to assist in the investigation of a crime or to prevent a crime or disorder by a CHIS who:

establishes or maintains a personal or other relationship with a person for the covert purpose of facilitating the doing of anything which is:

- covertly using a relationship to obtain information or to provide access to any information to another person or

- covertly disclosing information obtained by the use of such a relationship or as a consequence of the existence of such a relationship.

Members of the public volunteering information as part of their normal civic duties may, in some circumstances, be regarded as a CHIS.

The use of material which is obtained through covert surveillance either as a directed surveillance investigation/operation or through a CHIS can be used as evidence in criminal and civil proceedings.

Any material obtained through the course of the surveillance is subject to the ordinary rules for retention and disclosure of material under the Criminal Procedure and Investigation Act 1996.

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

## AUTHORISING OFFICER

Part II of RIPA 2000 permits a public authority to carry out surveillance provided proper procedures are followed.

An AO will be responsible for any surveillance either through an investigation or operation to be carried out or for the use of a CHIS.

It is an AO's responsibility to ensure that the forms have been completed properly.

It is fundamentally important that the AO is able to evidence the fact that he has read and considered each application and based his considerations upon the principles of necessity and proportionality. Obviously, it is a matter for the individual AO to decide how to demonstrate this effectively, bearing in mind that he or she could be called on to justify the considerations at a later date in court or at a tribunal hearing.

If necessary, the AO must challenge the officer as to the use of the authorisation if the AO considers:-

- that the correct procedures have not been followed properly,
- that an alternative method of obtaining the necessary information can be used,

- that a risk assessment has not been properly completed.

Authorising Officers should not be responsible for authorising investigations or operations in which they are directly involved.

A list of Authorising Officers is set out at **Appendix 1**. Where consideration is given to making an application for authorisation, general advice on procedures and on this Policy may be obtained from Legal Services (Billy Nanner) or from any of the Authorising Officers. In addition, each of those Council Departments without intra-departmental Authorising Officers has nominated at least one RIPA Liaison Officer who should also be informed about any proposed application. The RIPA Liaison Officer will maintain a good general awareness of RIPA 2000 by way of training and their involvement in the process will provide an additional means of ensuring compliance with the principles of necessity and proportionality. A list of RIPA Liaison Officers is set out at **Appendix 4**.

## COLLATERAL INTRUSION

The AO must take into account the risk of intrusion into the privacy of persons other than those who are direct subjects of the operational investigation such as innocent bystanders.

Measures must be taken wherever practical to avoid unnecessary intrusion into the lives of those not directly involved in the operation.

The application for authorisation should include an assessment of the risk of Collateral Intrusion and the Authorising Officer should consider this when assessing proportionality.

**RISK ASSESSMENT**

A risk assessment must be undertaken by the AO before authorisation is given in order to conduct the use of a CHIS. The risk assessment should concentrate on the security, safety and welfare of the CHIS in relation to what they are being asked to do.

**RIPA MONITORING OFFICER**

The Codes of Practice place certain responsibilities on the Senior Responsible Officer (RIPA Monitoring Officer). Code 3.22 states that "within every relevant public authority the SRO must be responsible for:-

- the integrity of the process in place within the Authority to conduct directed surveillance or acquire communications data
- compliance with the requirements of Statute or the Code
- oversight of the reporting of any errors relating to the acquisition of communications data to the Inspection of Communications Commissioner's Office
- the identification of any errors in the implementation of processes so as to minimize the repetition of errors
- engagement with the OSC and IOCCO Inspectors when they conduct their inspections
- where necessary to oversee the implementation of post Inspection Action Plans approved by the Commissioners

To ensure these requirements are met the RIPA Monitoring Officer (RMO) maintains oversight and quality control in relation to RIPA functions and processes. The RMO maintains the Central Record of Authorisations and is also responsible for RIPA training and the heightening of awareness of RIPA issues throughout the Council and an oversight of all applications to ensure ongoing quality control. The Council's RMO is Chrystal Wallage – Assistant Director of Finance (Audit).

**Set out below are the procedures for:**

- Directed Surveillance
- Covert Human Intelligence Source (CHIS)
- Communications Data

## PROCEDURE ON DIRECTED SURVEILLANCE

### The Grant of Authorisation

When considering a request for directed surveillance the AO must ensure that the authorisation is necessary for the purpose of preventing and detecting crime, or of preventing disorder[1].

The AO must believe that the surveillance is necessary and proportionate in order for this to be achieved.

The AO must give the authorisation in writing on the correct form – "**Authorisation Directed Surveillance**". The form is available on the Council's DNet.

If an urgent case requires an authorisation then it need not be in writing. However, as soon as practically possible the authorisation must be recorded in writing on the form.

The Authorising Officer passes the form (labelled "draft" at this stage) to a legal officer within the Director of Legal Services' Division for a "quality assurance check".

Following this (and subject to the quality assurance check/legal advice) the form is passed to Audit Services where a Unique Reference Number will be allocated from the central database also giving details of the date and type of authorisation, the subject of the surveillance, any surveillance equipment used and the name of the Authorising Officer for input on the central database.

At this stage all applications will be reviewed by the RIPA Monitoring Officer as a final quality check to ensure compliance with the Act and RIPA (Code of Practice Order) 2010. If any queries arise at this stage the application will be referred back to the AO.

Judicial Approval

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

[1] Footnote 33 of the Code states "preventing or detecting crime goes beyond the prosecution of offenders and includes actions taken to avert, end or disrupt the commission of criminal offences"

The judicial approval mechanism is in addition to the in-house authorisation process under the relevant parts of RIPA as outlined in the Codes of Practice and this Policy. The County Council's process for assessing necessity and proportionality, completing the RIPA authorisation/application form and seeking approval from an authorising officer/designated person will remain the same.

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

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

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

**Procedure for Applying for Judicial Approval**

**Making the Application**

Following approval by the authorising officer/designated person and after clearance by Legal Services and the Assistant Director of Finance (Audit) and RIPA Monitoring Officer, the first stage of the process is for the Assistant Director of Finance (Audit) and RIPA Monitoring Officer to contact the legal advisors at Her Majesty's Courts and Tribunals Service (HMCTS) at the magistrates' court to arrange a hearing.

The Assistant Director of Finance (Audit) and RIPA Monitoring Officer will provide the JP with a copy of the original RIPA authorisation or notice and the supporting documents setting out the case. This forms the basis of the application to the JP and **should contain all information that is relied upon**. For communications data requests the RIPA authorisation or notice may seek to acquire consequential acquisition of specific subscriber information. The necessity and proportionality of acquiring consequential acquisition will be assessed by the JP as part of his consideration.

The original RIPA authorisation or notice should be shown to the JP but will be retained by the County Council so that it is available for inspection by the

Commissioners' offices and in the event of any legal challenge or investigations by the Investigatory Powers Tribunal (IPT). The court may wish to take a copy.

In addition, the County Council will provide the JP with a partially completed judicial application/order form (see Appendix 6).

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

The order section of this form will be completed by the JP and will be the official record of the JP's decision. The County Council must:-

- obtain judicial approval for all initial RIPA authorisations/applications **and renewals,**
- retain a copy of the judicial application/order form after it has been signed by the JP.

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

**Arranging a Hearing**

HMCTS have agreed that, on receipt of a notification from the Assistant Director of Finance (Audit) and RIPA Monitoring Officer, either by telephone or e-mail, stating that the County Council has an application which requires approval they will attempt to ensure that the application is reviewed by the District Judge at the start of business on the following working day. It is therefore imperative that officers seeking approval allow sufficient time to accommodate this extended process.

On the rare occasions where out of hours access to a JP is required then it will be for the Assistant Director of Finance (Audit) and RIPA Monitoring Officer to make arrangements with the relevant HMCTS legal staff. In these cases the County Council will need to provide two partially completed judicial application/order forms so that one can be retained by the JP. The Authority should provide the court with a copy of the signed judicial application/order form the next working day.

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

## Attending a Hearing

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

The Code of Practice envisages that the case investigator (applicant) will be best placed to fulfil this role as they will know the most about the investigation and will have determined that use of a covert technique is required in order to progress a particular case. The SPoC (single point of contact) should attend hearings relating to applications for communications data RIPA authorisations or notices. This does not, however, remove or reduce in any way the duty of the authorising officer to determine whether the tests of necessity and proportionality have been met. Similarly, it does not remove or reduce the need for the forms and supporting papers that the authorising officer has considered and which are provided to the JP to make the case.

A list of those officers who may attend court in these circumstances is shown at Appendix 5.

## Decision

The JP will consider whether he or she is satisfied that at the time the authorisation was granted or renewed or the notice was given or renewed, there were reasonable grounds for believing that the authorisation or notice was necessary and proportionate. They will also consider whether there continues to be reasonable grounds. In addition they must be satisfied that the person who granted the authorisation or gave the notice was an appropriate designated person within the local authority and the authorisation was made in accordance with any applicable legal restrictions, for example that the crime threshold for directed surveillance has been met.

**The forms and supporting papers must, by themselves, make the case. It is not sufficient to provide oral evidence where this is not reflected or supported in the papers provided**. The JP may note on the form any additional information he or she has received during the course of the hearing but information fundamental to the case should not be submitted in this manner.

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

The JP will record his/her decision on the order section of the judicial application/order form. HMCTS administration will retain a copy of the

Authority's RIPA authorisation or notice and the judicial application/order form. This information will be retained securely.

The SPoC (Single Point of Contact) should be provided with a copy of the order to the communications service provider for all communications data requests and the County Council's SPoC Officer will not acquire the CD requested, either via the CSP or automated systems until the JP has signed the order approving the grant.

**Outcomes**

Following their consideration of the case the JP will complete the order section of the judicial application/order form (see form at Appendix 6) recording their decision. The various outcomes are detailed below:-

The JP may decide to:-

- **Approve the Grant or renewal of an authorisation or notice**
  The grant or renewal of the RIPA authorisation or notice will then take effect and the applicant may proceed to use the technique in that particular case,

- **Refuse to approve the grant or renewal of an authorisation or notice**
  The RIPA authorisation or notice will not take effect and the applicant may **not proceed with the course of action.**

- **Refuse to approve the grant or renewal and quash the authorisation or notice**
  This applies where a magistrates' court refuses to approve the grant, giving or renewal of an authorisation or notice and decides to quash the original authorisation or notice. The court must not exercise its power to quash that authorisation or notice unless the applicant has had at least 2 business days from the date of the refusal in which to make representations.

The original form, post judicial approval, is kept on a secure central register maintained by Audit Services; a copy of the form is returned to the Authorising Officer. The surveillance must not commence before this copy form is received by the AO who will then inform the person carrying out the surveillance.

The central database will also provide automatic reminders for reviews/renewals etc; it will be used to keep an effective audit trail of all authorisations and will be reconciled with relevant departments on a two monthly basis.

**Information to be provided in the Application for Authorisation**

All officers should note that where there is any confusion or uncertainty as to whether an application for authorisation needs to be produced the matter should be referred to the Assistant Director of Finance (Audit) and RIPA Monitoring Officer to ensure consistency and compliance with the requirements of the Act.

A written application for authorisation for directed surveillance must:-

- describe the conduct to be authorised,

- the purpose of the investigation or operation.

The application must include the following:-

- the reasons why the authorisation is sought.

- the grounds of the relevant operation or investigation i.e. for the purposes of preventing or detecting crime or disorder.[2][3]

- the reasons why the surveillance is considered proportionate to what it seeks to achieve.

- the nature of the surveillance.

- the identities where known of those to be the subject of the surveillance.

- an explanation of the information which is to be obtained as a result of the surveillance.

- details of any potential collateral intrusion and why the intrusion is considered to be justified.

- details of any confidential information that is likely to be obtained as a consequence of the surveillance.

- a subsequent record of whether authority was given or refused, by whom and the date and time.

In urgent cases where oral authorisation has been obtained, when the written authorisation is completed this should include the following:-

[2] Footnote 33 of the Code states "preventing or detecting crime goes beyond the prosecution of offenders and includes actions taken to avert, end or disrupt the commission of criminal offences"

[3] Applicants must always specify the crime or offence which is under investigation (including the relevant Section of the Act or legislation) as this is a key part of the necessity test. The Home Office and ACPO DCG guidance document provides clear guidance in this respect and is available on the County Council's website

- the reasons why the AO or the officer entitled to act in urgent cases considered the case so urgent that an oral instead of a written authorisation was given.

- the reasons why it was not reasonably practical for the application to be considered by an AO.

**Duration of Authorisation**

A written authorisation will cease to have effect at the end of the 3 month period from when it was obtained.

An urgent oral authorisation or written authorisation which has been obtained in an urgent case will cease to have effect after 72 hours from when it was obtained.

**Reviews of Authorisation**

Regular reviews of the authorisation must be undertaken to assess the need for the surveillance to continue. In each case the AO should decide how often a review should be undertaken. A review date should be recorded on the form when authorisation is granted. The review of any authorisation must be completed on the correct form – "**Review of a Directed Surveillance Authorisation**". The form is available on the Council's DNet. The original form should be forwarded to Audit Services who will keep it on a secure central register.

**Renewals of Authorisation**

If at any time before an authorisation would cease to have effect the AO considers it necessary for the authorisation to continue for the purpose for which it was given the AO may renew it in writing for a further period of 3 months. Renewals may also be granted orally in urgent cases for 72 hours.

All applications for renewal of authorisations for directed surveillance should include:-

- Whether this is the first renewal.

- Every occasion on which the authorisation has been renewed previously.

- Significant changes to the information relating to the conduct to be authorised and also the purpose of the investigation or operation.

- The reasons why it is considered to be necessary and proportionate to continue with the directed surveillance.

- The content and value to the investigation or operation of the information so far obtained by the surveillance and the result of regular reviews of the investigation operation

Authorisations may be renewed more than once and must be recorded as part of the central record of authorisations.

The correct form should be completed when applying for renewal of an authorisation –"**Renewal of a Directed Surveillance Authorisation**". The form is available on the Council's DNet. The original form should be forwarded to Internal Audit who will keep it on a secure central register.

**Cancellation of Authorisation**

The AO who granted or last renewed the authorisation must cancel that authorisation if he/she is satisfied that the surveillance no longer meets the criteria upon which it was authorised. This may be the result of a review.

Where the AO is no longer available this duty will fall on the person who is taking over the role of AO or any other designated AO within the Council.

The cancellation of surveillance must be completed on the correct form – "**Cancellation of a Directed Surveillance Authorisation**". The form is available on the Council's DNet. The original form should be kept on a secure central register maintained by Audit Services.

**Ceasing of Surveillance Activity**

As soon as the decision is taken that directed surveillance should be discontinued, instruction must be given to all those involved in the specific investigation or specific operation to stop all surveillance of the subject(s).

The date and time when an instruction was given to cease surveillance activity must be communicated to Internal Audit who will record this information in the central record.

**Central Record of all Authorisations**

A central record of all authorisations should be regularly updated whenever an authorisation is granted, renewed or cancelled. These records should be retained for at least three years from the ending of the authorisation and should contain the following:-

- The type of authorisation.

- The date of the authorisation.

- Name and rank of the Authorising Officer

- The Unique Reference Number (URN) of the investigation or operation.

- The title of the investigation or operation, including a brief description and names of subjects, if known.

- Details of any renewal of the authorisation.

- Whether the investigation or operation is likely to result in obtaining confidential information.

- The date the authorisation was cancelled.

- Full details of any equipment to be used.

In view of the content of the central record it clearly provides a comprehensive reference point in respect of each authorisation. It is also of great service in affording a quality control instrument for oversight purposes.

The Council should also maintain the following documentation (which need not form part of the central record):

- A copy of the application for authorisation.

- A record of the period over which surveillance took place.

- Details of any reviews.

- Copy of any renewal of authorisation.

## PROCEDURE FOR COVERT HUMAN INTELLIGENCE SOURCE (CHIS)

### Grant of an Authorisation

Under Part 2 RIPA 2000 Derbyshire County Council is provided with lawful authority to obtain authorisation to use a covert human intelligence source to assist in the investigation of an operation to detect or prevent a crime or disorder.

Where an AO considers a request to use a CHIS for a specific operation/investigation, the AO must believe that the authorisation is necessary for the purpose of preventing and detecting crime, or of preventing disorder. The AO must also believe the activity is proportionate to the likely outcome.

When undertaking an operation with a CHIS Derbyshire County Council will be subject to Article 8 of the European Convention on Human Rights and the Human Rights Act 1998.

When obtaining an authorisation the AO must ensure that the authorised use or conduct of the CHIS is a justifiable interference with an individual's rights under the Human Rights Act 1998.

The AO must balance the intrusiveness of the use of the CHIS against those being investigated and others who may be affected by the use of a CHIS in all circumstances.

The AO must believe that use of a CHIS is necessary and proportionate.

The AO must give the authorisation in writing on the correct form – "**Application for Authorisation of the Conduct or use of a CHIS**". The form is available on the Council's DNet. The original form should be forwarded to Audit Services who will keep it on a secure central register.

The AO passes the form (labelled "draft" at this stage) to a legal officer within the Director of Legal Services' Division for a "quality assurance check".

Following this (and subject to the quality assurance check/legal advice) the form is passed to Audit Services where a unique reference number will be allocated from the central database also giving details of the date and type of authorisation, the subject of the surveillance, any surveillance equipment used and the name of the Authorising Officer for input on the central database.

The original form is kept on a secure central register maintained by Audit Services; a copy of the form is returned to the Authorising Officer. The surveillance should not commence before the form is returned to the Authorising Officer who will then inform the person carrying out the surveillance.

**Information to be provided in the Application for Authorisation**

A written application for authorisation for the use of a CHIS must include the following:-

- The reasons why the authorisation is necessary and the grounds (preventing or detecting crime or disorder).
- Why the authorised conduct or use of a source is proportionate to what it seeks to achieve.
- The purpose for which the source will be deployed.
- Details of the investigation or operation and the nature of what the source will be asked to do.
- The level of authority required.
- Details of any potential collateral intrusion.
- Details of any confidential information likely to be obtained.

In urgent cases, the authorisation should record the reasons why the Authorising Officer considered the case so urgent that oral authorisation was given instead of written authorisation; and/or the reasons why it was not reasonably practicable for the application to be considered by the Authorising Officer. For oral authorisations the above details should be recorded in writing by the Applicant as soon as possible.

An AO may not grant an authorisation for the conduct or use of a CHIS unless he believes that arrangements exist to ensure there must be adequate records relating to the CHIS containing particulars of certain matters. Those matters are specified in the Regulation of Investigatory Powers (Source Records) Regulations 2000; Statutory Instrument 2000 No. 2725:-

- The source's identity.
- The identity, where known, used by the source.
- Any relevant investigating authority other than the Council maintaining the records.
- The means by which the source is referred to within each relevant investigating authority.
- Any other significant information in relation to the security and welfare of the source.
- Any confirmation made by a person granting or renewing an authorisation for the conduct or use of a source that the

information in relation to the means by which the source is referred to has been considered and any identified risks to the source have been properly explained to the source.

- The date and circumstances when and in which the source was recruited.

- The identities of those with management responsibilities for the source as mentioned in Section 29 (5)(a) to (c) of RIPA 2000.

- The period during which those persons mentioned above have discharged those responsibilities.
- The tasks given to the source.

- All communications between the source and a person acting on behalf of the Council.

- The information obtained by the Council in relation to the conduct or use of a source.

**Judicial Approval**

For the process to be followed in respect of Judicial Approval which is required under the Protection of Freedoms Act 2012 – Changes to Provisions Under the Regulation of Investigatory Powers Act 2000 (RIPA) please refer to the detailed procedures at pages 9 to 13 above.

**Duration of Authorisation**

A written authorisation which has been granted by an AO for the use of a CHIS will cease to have effect at the end of a 12 month period from the day that it took effect.

**Reviews of Authorisation**

Regular reviews of the authorisation must be undertaken to assess the need for the use of a source to continue. The review should include the use made of the source, the tasks given and the information obtained. In each case the AO should decide how often a review should be undertaken. A review date should be recorded on the form when authorisation is granted. The review of any authorisation must be completed on the correct form – "**Review of a CHIS Authorisation**". The form is available on the Council's DNet. The original form should be forwarded to Audit Services who will keep it on a secure central register.

**Renewal of Authorisation**

If at any time before an authorisation would cease to have effect the AO considers it necessary for the authorisation to continue for the purpose for

which it was given, the AO may renew it in writing for a further 12 months. Renewals may also be granted orally in urgent cases for 72 hours. There must be a documented review before renewal.

- All applicants for renewal of authorisations for the use of a CHIS should include:-

- Whether this is the first renewal.

- Every occasion on which the authorisation has been renewed previously.

- Significant changes to the information relating to the conduct to be authorised and also the purpose of the investigation or operation.

- The reasons why it is considered to be necessary and proportionate to continue with the use of the CHIS.

- Details of the use of the CHIS since the grant of the authorisation/renewal.

- The task given to the CHIS during that period and the information obtained from that conduct.

- Details of the results of the regular reviews.

- Details of the review of the risk assessment.
- The AO's comment and statement to the continued or discontinued use of the CHIS.

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

The correct form should be completed when applying for renewal of an authorisation – "**Application for Renewal of a CHIS**". The form is available on the Council's DNet. The original form should be forwarded to Audit Services who will keep it on a secure central register.

**Cancellation of Authorisation**

The AO who granted or last renewed the authorisation must cancel that authorisation if he is satisfied that the use of the CHIS is no longer necessary.

An explanation as to the value of the CHIS will need to be included.

Where the AO is no longer available this duty will fall on the person who is taking over the role of AO or other designated AO.

The cancellation of the use of a CHIS must be completed on the correct form – "**Cancellation of an Authorisation for the use or Conduct of a CHIS**". The form is available on the Council's DNet. The original form should be forwarded to Audit Services who will keep it on a secure central register.

**Ceasing of Surveillance Activity**

As soon as the decision is taken that the use of a CHIS is to be discontinued instruction must be given to all those involved in the specific investigation or specific operation.

The date and time when an instruction was given on the ceasing of the use of a CHIS must be communicated to Audit Services who will record this information in the central record.

**Managing your CHIS**

Provision is made in Section 29(5) of RIPA 2000 for a CHIS to be carefully managed.
An officer within the Council following authorisation is to have day-to-day responsibility for dealing with the source on behalf of the Council and:-

- Directing the source's activities.

- Recording information supplied by the source.

- Monitoring the welfare and security of the source.

- Maintaining a record of the use made of the source

Another officer within the Council is to have general oversight of the use made of the source.

A risk assessment must be carried out in relation to what issues could be facing the security and welfare of a CHIS in relation to what they are to be tasked to do. This should take place before any authorisation is granted and at any renewal, review and cancellation.

Special safeguards are in place for vulnerable individuals or juveniles. The first is someone who is or may be in need of community care because of disability, age or illness and may need protecting from exploitation. They should only be used as sources in exceptional cases. The second is a young person under 18. Those under 16 cannot be used as a source against their parents or anyone with parental responsibility for them. Juveniles can only be authorised as sources for 1 month. Only the Head of Paid Service (in his absence the Deputy) can authorise use of a CHIS involving the use of a juvenile or vulnerable individual.

## Central Record of all Authorisations

A central record of all authorisations should be regularly updated whenever an authorisation is granted, renewed or cancelled. These records should be retained for a period of at least three years from the ending of the authorisation.

Records must be kept of the authorisation and use of a source. Also, records or copies of the following should be kept by the Council:-

- A copy of the authorisation.

- A copy of any renewal and the reason why it was considered necessary to renew the authorisation.

- Any authorisation granted or renewed orally and the reason for this.

- Any risk assessment made in relation to the source.

- Circumstances of tasks given to the source.

- The value of the source to the Council.

- Details of reviews and/or cancellation of authorisation.

- Date and time of any instruction given by the Authorising Officer to cease use of a source.

In view of the content of the central record, it clearly provides a comprehensive reference point in respect of each authorisation. It is also of great service in affording a quality control instrument for oversight purposes.

## Access to Communications Data (RIPA Part 1 Chapter II)

## ACQUISITION AND DISCLOSURE OF COMMUNICATIONS DATA

### Access to Communication Data

In addition, local authorities investigating criminal offences now have powers (by virtue of the Regulation of Investigatory Powers (Communications Data) Order 2004 ("the Order") to gain access to communications data – that is, information held by telecommunication or postal service providers about the use of their services by persons who are the subject of criminal investigations.

In using such powers, officers must have full regard to the Acquisition and Disclosure of Communications Data Code of Practice. As with covert surveillance, access to communications data must be authorised by a 'Designated Person' and obtained via the Council's 'Single Point of Contact' (SPOC).

Communications data is information held by communication service providers (e.g. telecom, internet and postal companies). The Act makes provision for obtaining communications data from such service providers and the disclosure to any person of such data. Communications data includes information relating to the use of a postal service or telecommunication system but **does not include** the contents of the communication itself.

As with surveillance above, any such interference must be:-

- lawful and
- necessary and
- proportionate

AND any such Authorisations for access to communications data may only be granted if the Designated Person believes that such authorisation is necessary for the prevention or detection of crime or preventing disorder {The Regulation of Investigatory Powers (Communications Data) Order 2010}. Detecting crime includes establishing by whom, for what purpose, by what means and generally in what circumstances any crime was committed, the gathering of evidence for use in legal proceedings and the apprehension of the person (or persons) by whom any crime was committed.

In addition, as previously explained, the risk of collateral intrusion must be considered and justified.

### Categories of Communications Data

There are three broad areas of communications data, only two of which can be accessed by this Council. They are as follows:-

Section 21(4)(b) Service Data – this is information held by a telecom or postal service provider about the use made of a service by a person under investigation such as:

- Outgoing calls on a landline telephone or contract or prepay mobile phone.
- Timing and duration of service usage.
- Itemized connection records.
- Internet logon history.
- E-mails (sent).
- Information about the connection, disconnection and reconnection of services.
- Information about the provision of conference calling, call messaging, call waiting and call barring.
- Information about the provision and use of forwarding/redirection services (postal and telecom).
- Information about selection of preferential numbers or discount calls.
- Records of postal items e.g. records of registered/recorded/special delivery postal item, records of parcel consignment/delivery/collection.

Section 21(4)(c) Information about Communication Service users (“Subscriber data”) such as:-

- Name of account holder/subscriber (also known as “reverse look ups”).
- Installation and billing addresses.
- Method of payment/billing arrangements.
- Collection/delivery arrangements for a PO Box (i.e. whether it is collected or delivered – not where it is collected from or delivered to).
- Information about apparatus used by or made available to the account holder/subscriber including the manufacturer, model etc.
- Other customer information e.g. account notes, demographic information or sign up data (not passwords or personalised access information).

**Local Authorities are NOT authorised to obtain access to "traffic data" i.e. information that identifies any person, equipment, location to or from which a communication is or may be transmitted.**

Further, these powers do not permit access to the **contents** of the communication itself.

**Organisations from which local authorities may access Communications Data**

All Communications data is accessed from Communication Service Providers (CSPs). These may be:-

- **Telecom Providers,**

  Mobile phone service providers, landline phone service providers or International Simple Voice Resellers.

- **Internet Providers**

  ISPs, Virtual ISPs and Portals

- **Postal Providers**

**The SPOC**

Integral to the acquisition of communications data under RIPA is the single Point of Contact (SPOC). The Home Office Code of Practice recommends that all authorities who use these powers have a SPOC. All Accredited Officers within the SPOC must attend a Home Office approved course. On passing the examination at the end of the course, Accredited Officers are granted a unique PIN reference number and added to the Home Office list of Authorising Officers. In addition, the Accredited Officer must keep abreast of the law relating to, and developments within, the communications industry.

This system aims to provide an efficient regime, as the SPOC will ensure consistency in dealing with the postal or telecommunications operator on a regular basis, the Council will be able to regulate itself, and it will help reduce the burden on the postal and telecommunications operator.

**This policy requires that the roles of Accredited Officer and Designated Person are carried out by different individuals.**

The Accredited Officers at Derbyshire County Council are contained in **Appendix 2**.

**Responsibilities and Role of the Accredited Officer**

The Accredited Officer has the following duties:-

- To assess whether access to communications data in a particular case is reasonably practical for the CSP.

- To advise investigators and Designated Persons on the practicalities of accessing different types of communications data from different Communication Service Providers (CSPs).

- To advise investigators and Designated Persons on whether specific communications data falls under Section 21(4)(b) or 21(4)(c) of RIPA.

- To assess any cost and resource implications for both the Council and the CSP.

- To provide a safeguard for CSPs that authorisations and notices are authentic.

- To retain records of all applications, Authorisations and Notices.

- To retain a record of the dates on which Authorisations and Notices are started and cancelled.

- To retain all Applications in the event that there may be a complaints Tribunal.

- To retain a record of any errors that may have occurred in the granting of Authorisations, or issuing of notices, and provide an explanation to the Interception of Communications Commissioner.

- To maintain a SPOC log sheet for each application they are involved in.

The Accredited Officer will assess the application and in particular whether the request has been made properly and whether the required communications data can reasonably be obtained together with any adverse cost or resource implications and forward a copy of the Application for consideration by the Designated Person together with the Notice/Authorisation (see below) for signature.

**The Designated Person**

A Designated Person is someone holding a prescribed office, rank or position within a local authority and has been designated for the purposes of acquiring communications data by the Order.

A Designated Person must be a Director, Head of Service, a Service Manager or equivalent and must have current working knowledge of human rights principles. The Designated Persons for the purposes of Part 1 Chapter II RIPA are contained in **Appendix 3**.

## Responsibilities of Designated Persons

Designated persons must ensure that requests for Communications Data are both necessary and proportionate prior to granting an Authorisation or giving a Notice.

Designated persons should not be responsible for granting authorisations or giving notices in relation to investigations or operations in which they are directly involved (unless it is necessary to act urgently).

They have a duty to consider various points, as follows:-

- Whether the case justifies the accessing of Communications Data under Section 22(2)(b) i.e. that it is for the prevention or detection of crime or preventing disorder[4].

- Whether obtaining access to the data by the conduct authorised by the authorisation, or required of the CSP in the case of a Notice, is proportionate to what is sought to be achieved.

  *As with surveillance, access to communications data should only be authorised by the Designated Person where it is considered to be necessary and proportionate to the objectives the Council is seeking to achieve i.e. it should be no more than required in the circumstances, should not be arbitrary and should balance the extent of the intrusion or the interference with the individual's private life against the benefit to be achieved by the operation and the public interest.*

- Whether the circumstances of the case still justify such access in cases where there is likely to be collateral intrusion.

  *Collateral intrusion (as defined above) should also be considered and any application should highlight the potential for infringement of the privacy of third parties.*

- Whether any urgent timescale is justified.

## Advice to assist Designated Persons with their written considerations

*It is fundamentally important that Designated Persons ("DP") must be able to evidence the fact that they have read and considered each application and based their considerations upon the principles of necessity and proportionality. Obviously, it is a matter for the individual DP to decide how to demonstrate this effectively, bearing in mind that he or she could be called upon to justify the considerations at a later date in Court or at a Tribunal hearing. It may well be appropriate in some cases to merely record the fact that the DP has read*

[4] Footnote 33 of the Code states "preventing or detecting crime goes beyond the prosecution of offenders and includes actions taken to avert, end or disrupt the commission of criminal offences"

*and considered the application and that he or she believes that obtaining the data in question is necessary and that obtaining the data by the conduct is proportionate to what is sought to be achieved by obtaining the data or words to that effect. This would largely depend upon the quality of the application and whether the DP is fully satisfied that the applicant has made out a strong case in all respects.*

*In practice, the standard of applications will vary according to the knowledge and experience of the applicant and, therefore, the DP will often be required to make a more detailed judgement. Equally, it may be that the application is quite complex or that it requests a particularly intrusive set of data in which case the DP may wish to address this specifically. The DP's comments should be specific to the application in question. For example, the grade of the application and what the AO has advised in relation to the feasibility and the conduct of retrieving data. The DP may also be able to make a comment upon the wider strategic objective in arriving at a decision and stating that he or she has examined the Authorisation and or Notice.* ***For these reasons it is recommended that the DP should tailor the comments to the individual application as this is the best means of demonstrating that it has been properly considered.***

## PROCEDURE FOR *APPLYING FOR* COMMUNICATIONS DATA

All requests to obtain communications data must be made in writing by the Accredited Officer on the "**Application for Communications Data**" form. The form is available on the Council's DNet.

All such requests must include the following information:-

- Name or designation of the officer requesting the communications data.
- The operation and person (if known) to which the requested data relates.
- A description of the data requested and where appropriate time periods.
- Identification of the section of the Act the communication data is covered by.
- Reasons why obtaining the data is considered to be necessary **N.B. <u>there is only one reason – for the prevention or detection of crime or preventing disorder,</u>**
- An explanation as to why obtaining the data is considered to be proportionate to what it seeks to achieve.
- An indication (where appropriate) that the matter of collateral intrusion has been considered.
- The timescale within which the data is required.

### Advice to assist Accredited Officers with completion of the application form

*In the 'necessity' section of the application Applicants must ensure that they always specify the particulars of the crime under investigation including the relevant section of the Act or legislation, as this is a key part of the necessity test. Applicants should refer to the Home Office and ACPO DCG guidance document which is available on DNet. In essence necessity should be a short explanation of the crime, the suspect/trader, victim or witness and the phone or communications address and how all these three link together. The source of the telephone number or communications address should also be outlined. For example, if the number was obtained from a complainant or business flyer this should be outlined.*

*The proportionality section should give an explanation as to why specific date/time periods of data have been requested (how these are proportionate) and what the applicant expects to achieve from obtaining the data. Proportionality should explain how the level of intrusion is justified when taking into consideration the benefit the data will give to the investigation. It may be*

*pertinent to outline what other less intrusive methods/checks have already been tried to e.g. trace an unknown trader. For example, if the applicant had tried to telephone the number and speak to the user of the phone, or why this method was not deemed feasible or had failed. An explanation of what is going to be done with the communications data once it is acquired and how the action will benefit the investigation will assist with the justification of proportionality.*

*In the collateral intrusion section of the form it is important for the applicant to consider what collateral intrusion may occur as a result of the specific request and how this will be managed or how certain actions will reduce the potential for collateral intrusion. In other words, applicants should state whether they are likely to obtain data which is outside the realm of their investigation and outline their plans for managing it. Although collateral intrusion is generally minimal on a subscriber check, if is still important for the applicant to consider what collateral intrusion may occur as a result of their request. (In a lot of cases, the suspect/trader will be contacted on the actual telephone number by the complainant and therefore this reduced the potential for collateral intrusion). Applicants should also mention whether it is known that the telephone number (or other type of data) has been used to advertise the business, either in the press/internet or on business cards/flyers, as this would also be good evidence to show that the trader/suspect is actually using the telephone number and further reduce the potential for collateral intrusion.)*

**Processing the Application**

Completed application forms are assessed by an Accredited Officer. The Accredited Officer then passes the form to the Designated Person (together with the draft Notice/Authorisation) to approve the Application. The Designated Person will consider whether the proposed conduct is necessary and proportionate and will authorise the conduct if satisfied on these points.

The Designated Person passes the form (labelled “draft” at this stage) to a legal officer within the Director of Legal Services’ Division for a “quality assurance check”.

Following this (and subject to the quality assurance check/legal advice if taken) the form is passed to the Central SPOC in Audit Services who will allocate a unique reference number, update the central database and acquire the data (ie issue the Appropriate Notice to the Communications Service Provider or retrieve the data itself by virtue of the Authorisation) and supply it to the Applicant.

Each SPOC will maintain a SPOC log sheet for each application they are involved in.

The original form is kept on a secure central register maintained by Audit Services; a copy of the form is returned to the Applicant.

At this stage all applications will be reviewed by the RIPA Monitoring Officer as a final quality check to ensure compliance with the Act and RIPA (Code of Practice Order) 2010. If any queries arise at this stage the application will be referred back to the AO.

**Judicial Approval**

For the process to be followed in respect of Judicial Approval which is required under the Protection of Freedoms Act 2012 – Changes to Provisions Under the Regulation of Investigatory Powers Act 2000 (RIPA) please refer to the detailed procedures at pages 9 to 13 above.

**Procedure for obtaining Communications Data**

Under RIPA, there are two permissible ways of accessing Communications Data both of which must be channelled through the SPOC. The Order permits access to communications via an 'authorisation' under Section 22(3) of RIPA that allows the Council to collect or retrieve the data itself from the service provider, or a 'Notice' under Section 22(4) given by the Council to a postal or telecommunications operator
and requires that operator to collect the data and provide it to the Council.

In the vast majority of cases, communications data will be obtained via the **Notice** procedure (see below). Only in exceptional circumstances, will an **Authorisation** be appropriate to allow the Council to retrieve the data itself i.e. where the service provider is not capable of retrieving the data, where the investigation would be prejudiced if the service provider retrieves the data, and where a prior agreement is in place between the Council and the relevant service provider(s) as to the appropriate mechanisms for the disclosure of communications data. (There are currently no such agreements in place).

Oral applications for communications data are not permitted.

**Notice under Section 22(4)**

The Notice is available on the Council's DNet.

A Notice is where a CSP collects data on behalf of the Council. The form of Notice must include the following information:

- A description of the data required (and whether it is Communications Data under Section 21(4)(b) or Section 21(4)(c) of the Act.

- The purpose for which the data is required. **This will always be for the prevention or detection of crime or preventing disorder.**

- The name (or designation) and office, rank or position of the Designated Person.
- The manner in which the data should be disclosed.

- A unique reference number.

- If relevant, any indication or urgency.

- A statement setting out that data is sought under the provisions of Part I, chapter II of the Act.

- Contact details.

The Notice must also be approved by the Designated Person, dated, timed and signed before it can be served on the service provider. Once this has been done, the Central SPOC in Audit Services will serve the Notice on the service provider. When data is provided, the Central SPOC will then feed it back to the Applicant.

Derbyshire County Council's Accredited Officers will use the template Notice available on the Home Office Website.

**Authorisation under Section 22(3)**

An Authorisation is used by the Council collecting or retrieving the Communications Data itself. It may only be given in these circumstances:-

- When the Postal or Telecommunications Operator is not capable of obtaining or retrieving the communications data.

- When it is believed that the investigation may be prejudiced if the Postal or Telecommunications Operator is asked to collect the data itself.

- When there is a prior agreement in place between the Council and the Postal or Telecommunications Operator as to the appropriate mechanisms for the disclosure of Communications Data.

Each Authorisation must include the following information:-

- A description of the conduct that is authorised.

- A description of the Communications Data required (identify whether it is Communications Data under Section 21(4)(b) or 21(4)(c) of the Act).

- Identify the purpose for which the data is required. **This will always be for the prevention or detection of crime or preventing disorder.**

- The name (or designation) and office, rank or position of the Designated Person.

- A unique reference number.

A Designated Person may only authorise persons working in the same local authority to engage in specific conduct to obtain communications data. This will normally be the Central SPOC in Audit Services. They must be cancelled by the Designated Person as soon as they are no longer considered to be either necessary or proportionate.

Authorisations are valid for one month, but can be renewed using the appropriate form for a period of up to one month.

**Urgent Release**

An application for Communications Data may only be made and approved orally, on an urgent basis, where it is necessary to obtain Communications Data in an emergency i.e. where life would be endangered or the investigation jeopardised. Urgent oral authorisations have a duration period of 72 hours commencing from the time when the authorisation was originally granted.

Written notice must be given to the CSP retrospectively within one working day of the oral notice being given. Failure to do so will constitute an error reportable to the Commissioner.

Following this, the Accredited Officer will compile a written report containing details of all contemporaneous records relating to the circumstances leading up to the matter of urgency and the reason for the decision made.

**Duration of Notices and Authorisations**

Notices and Authorisations will only be valid for **one month**. This period will begin when the Notice is given or the Authorisation granted.

All Notices and Authorisations should refer expressly to the acquisition of data relating to a specific date or period. Where the data required is specified as "current" the relevant date taken will be the date of the Notice or Authorisation. For the obtaining of communications data that will be generated in the future, disclosure may only be required of data obtained by the postal or telecommunications operator **within** this period i.e. up to one month. For 'historical' Communications Data disclosure may only be required if in the possession of the postal or telecommunications operator. The Designated Person should give particular regard to the period of time that they are requesting data for and specify the shortest period in which the objective for which the data is sought can be achieved. To do otherwise would impact on the proportionality requirements and impose an unnecessary burden on CSP's.

**Renewal of Notices and Authorisations**

A Notice or Authorisation may be renewed at any time during the month it is valid for for a period of up to one month, by following the same procedure as

in obtaining a fresh Notice or Authorisation. The Renewal takes effect at the point at which the Notice or Authorisation it is renewing expires.

Authorisation of Renewals will normally be made by the original Designated Person provided that there is a continuing requirement to acquire or obtain data that may be generated in the future and that the application continues to meet the original criteria for granting.

**Cancellations of Notices and Withdrawal of Authorisations**

When an application for communications data is made the Applicant undertakes to inform the Accredited Officer of any change in circumstances that no longer justifies the acquisition of the data. Any such changes in circumstances should be brought to the attention of the Designated Person.

The Designated Person should cancel a Notice or withdraw an Authorisation as soon as it is no longer necessary or the conduct is no longer proportionate to what is sought to be achieved. The duty to cancel a Notice or withdraw an Authorisation primarily falls on the Designated Person or on that person's behalf on the Central SPOC in Audit Services. The cancellation or withdrawal must be in writing.

**Keeping Records**

Applications, copies of Notices and records of the withdrawal of Authorisations and the cancellation of Notices must be retained in written or electronic form and physically attached or cross-referenced where they are associated with each other. Records must be held centrally by the Central SPOC in Audit Services.

These records must be available for annual inspection by the Interception of Communications Commissioner.

**The Senior Responsible Officer/RIPA Monitoring Officer**

The Codes of Practice place certain responsibilities on the Senior Responsible Officer (RIPA Monitoring Officer). Code 3.22 states that "within every relevant public authority the SRO must be responsible for:-

- the integrity of the process in place within the Authority to conduct directed surveillance or acquire communications data
- compliance with the requirements of Statute or the Code
- oversight of the reporting of any errors relating to the acquisition of communications data to the Inspection of Communications Commissioner's Office
- the identification of any errors in the implementation of processes so as to minimize the repetition of errors
- engagement with the OSC and IOCCO Inspectors when they conduct their inspections

- where necessary to oversee the implementation of post Inspection Action Plans approved by the Commissioners

To ensure these requirements are met the RIPA Monitoring Officer (RMO) maintains oversight and quality control in relation to RIPA functions and processes. The RMO maintains the Central Record of Authorisations and is also responsible for RIPA training and the heightening of awareness of RIPA issues throughout the Council and an oversight of all applications to ensure ongoing quality control. The Council's RMO is Chrystal Wallage – Assistant Director of Finance (Audit).

## CODE OF PRACTICE

The Regulation of Investigatory Powers Act 2000 Consolidating Orders and the new Codes of Practice for Covert Surveillance and Property Interference and Covert Human Intelligence Source (CHIS) came into force on 6th April 2010. These revised Codes, together with those covering the acquisition of communications data, can be obtained from the following url http://www.homeoffice.gov.uk/counter-terrorism/regulation-investigatory-powers/ripa-codes-of-practice/ which provide guidance on the proper application of the legislation and may be used as a source of reference.

The Protection of Freedoms Act 2012 – changes to provisions under the Regulation of Investigatory Powers Act 2000 (RIPA) Home Office guidance to local authorities in England and Wales on the judicial approval process for RIPA and the crime threshold for directed surveillance provides further guidance on this process and can be obtained from the following url http://www.homeoffice.gov.uk/publications/counter-terrorism/ripa-forms/local-authority-ripa-guidance/local-authority-england-wales?view=Binary

### What do the codes say?

The codes of practice provides detailed information about the responsibilities of each party involved in undertaking directed surveillance or accessing and disclosing communications data. It features specific guidance on:-

- Situations where the authorisation of directed surveillance or acquisition of communications data is considered necessary and proportionate.
- Grounds on which each relevant public authority can and cannot undertake such activities.
- When to grant authorisations, when to issue Notices.
- Duration, renewal and cancellation of authorisations and Notices.
- Record keeping.
- Data Protection.

Complaints about improper acquisition and disclosure of communications data may be reported to the Interception of Communications Commissioner who may then refer the case to the Investigatory Powers tribunal or they may be reported directly by an effected individual to the Tribunal at:-

Investigatory Powers Tribunal
PO Box 33220
London
SW1H 9ZQ

Telephone:- 020 7035 3711

November 2012

## APPENDIX 1

## LIST OF AUTHORISING OFFICER POSTS (subject to review)

## FOR DIRECTED SURVEILLANCE/CHIS

**Chief Executives/Corporate Resources**

Carl Hardman : Audit Services Manager

**Cultural and Community Services**

Martyn Smith : Deputy Head of Trading Standards

Graham Morgan : Trading Standards Manager

## APPENDIX 2

## ACCREDITED OFFICERS – ACCESS TO COMMUNICATIONS DATA

### Chief Executives/Corporate Resources

Carl Hardman : Audit Services Manager

### Cultural and Community Services

Graham Morgan : Trading Standards Manager

## APPENDIX 3

## DESIGNATED PERSONS – ACCESS TO COMMUNICATIONS DATA

### Chief Executives/Corporate Resources

Chrystal Wallage : Assistant Director of Finance (Audit) and RIPA Monitoring Officer (Head of Audit Services)

### Cultural and Community Services

Martyn Smith : Deputy Head of Trading Standards

## APPENDIX 4

## RIPA LIAISON OFFICERS

### Environmental Services

Stephen Kirkland : Business Manager - Highways

Denis Canney : Team Leader Planning Control - North

### Children & Younger Adults

Ian Johnson : Deputy Strategic Director

### Adult Care

Mary McElvaney : Assistant Director

## APPENDIX 5

## OFFICERS NOMINATED TO ATTEND COURT TO OBTAIN JUDICIAL APPROVAL

**Cultural and Community Services - Trading Standards**

| | | |
|---|---|---|
| Simon Kirk | : | Principal Trading Standards Officer |
| Ian Howarth | : | Principal Trading Standards Officer |
| Cory Walker | : | Senior Trading Standards Officer |
| Karen Bailey | : | Senior Trading Standards Officer |

**Chief Executives and Corporate Resources - Audit Services**

| | | |
|---|---|---|
| Carl Hardman | : | Audit Services Manager and SPOC Officer |
| Philip Spencer | : | Principal Auditor & IT Manager |
| Daniel Ashcroft | : | Principal Auditor & Projects Manager |

**Children & Younger Adults**

| | | |
|---|---|---|
| Sara Bartlet | : | Operations Manager (Safeguarding) |

**Adult Care**

| | | |
|---|---|---|
| Mary McElvaney | : | Assistant Director |
| Julie Heath | : | Group Manager |
| Rob Moore | : | Group Manager |

# APPENDIX 6

# JUDICIAL APPLICATION/ORDER FORM

**Application for judicial approval for authorisation to obtain or disclose communications data, to use a covert human intelligence source or to conduct directed surveillance. Regulation of Investigatory Powers Act 2000 sections 23A, 23B, 32A, 32B.**

Local authority:.....

Local authority department:.....

Offence under investigation:.....

Address of premises or identity of subject:.....

.....

.....

Covert technique requested: (tick one and specify details)

**Communications Data** ☐

**Covert Human Intelligence Source** ☐

**Directed Surveillance** ☐

Summary of details

.....

.....

.....

.....

.....

.....

**Note:** this application should be read in conjunction with the attached RIPA authorisation/RIPA application or notice.

Investigating Officer:.....

Authorising Officer/Designated Person:.....

Officer(s) appearing before JP:.....

Address of applicant department:.....

.....

Contact telephone number:.....

Contact email address (optional):.....

Local authority reference:.....

Number of pages:.....

18

**Order made on an application for judicial approval for authorisation to obtain or disclose communications data, to use a covert human intelligence source or to conduct directed surveillance. Regulation of Investigatory Powers Act 2000 sections 23A, 23B, 32A, 32B.**

Magistrates' court:.....

Having considered the application, I (tick one):

☐ am satisfied that there are reasonable grounds for believing that the requirements of the Act were satisfied and remain satisfied, and that the relevant conditions are satisfied and I therefore approve the grant or renewal of the authorisation/notice.

☐ refuse to approve the grant or renewal of the authorisation/notice.

☐ refuse to approve the grant or renewal and quash the authorisation/notice.

Notes

.....

.....

.....

.....

.....

Reasons

.....

.....

.....

.....

.....

.....

Signed:

Date:

Time:

Full name:

Address of magistrates' court:

19