RUSHCLIFFE BOROUGH COUNCIL

REGULATION OF INVESTIGATORY POWERS

ACT 2000 (RIPA)

POLICY AND GUIDANCE

CONTENTS

Revised: July 2006
October 2006
April 2009
Nov 2009; May ’10;

Nov 2012, NOV 2013, JUNE 2016

RUSHCLIFFE BOROUGH COUNCIL

POLICY ON REGULATION OF INVESTIGATORY POWERS ACT 2000 (RIPA)

Introduction

Rushcliffe Borough Council only carries out covert surveillance where such action is justified and endeavours to keep such surveillance to a minimum. It recognises its obligation to comply with RIPA when such an investigation is for one of the purposes set out in that Act and has produced a Guidance document to assist officers.

The Council acknowledges that the 2000 Act provides a statutory framework under which covert surveillance (referred to in the Act as directed surveillance or use of covert human intelligence sources – CHIS) can be authorised and conducted compatibly with human rights legislation.

Applications for authority

A senior officer authorised by the Council will consider all applications for authorisation in accordance with RIPA. Any incomplete or inadequate application forms will be returned to the applicant for amendment. The authorising officer shall in particular ensure that:-

- there is a satisfactory reason for carrying out the surveillance
- the serious crime threshold is met
- the covert nature of the investigation is necessary
- proper consideration has been given to collateral intrusion
- the proposed length and extent of the surveillance is proportionate to the information being sought
- Chief Executive's authorisation is sought where confidential legal/journalistic/medical/spiritual welfare issues are involved
- the authorisations are reviewed and cancelled
- records of all authorisations are sent to the Council's Solicitor for entry on the Central Register

- once authorisation has been obtained from the authorising officer the Investigating Officer will attend the magistrates' court in order to obtain judicial approval for the authorisation.

Training

Each Executive Manager shall be responsible for ensuring that relevant members of staff are aware of the Act's requirements. The Monitoring Officer shall ensure that all Authorising Officers have received appropriate training and that refresher training is provided from time to time.

Central register and records

The Monitoring Officer shall retain the Central Register of all authorisations issued by Rushcliffe Borough Council. The Senior Solicitor will also monitor the content of the application forms and authorisations to ensure that they comply with the Act.

Scrutiny

The Council has appointed the Monitoring Officer as the Senior Responsible Officer (SRO).

Further details of the role of the SRO and the role of elected members is set out in Appendix A.

June 2016

REGULATION OF INVESTIGATORY POWERS ACT 2000 (RIPA)

GUIDANCE – PART I

DIRECTED SURVEILLANCE

1. **Purpose**

The purpose of this guidance is to explain

the scope of RIPA – Part II
the circumstances where it applies, and
the authorisations procedures to be followed

2. **Introduction**

2.1 This Act, which came into force in 2000, is intended to regulate the use of investigatory powers exercised by various bodies including local authorities, and ensure that they are used in accordance with human rights. This is achieved by requiring certain investigations to be authorised by an appropriate officer and approved by the judiciary before they are carried out.

2.2 The investigatory powers, which are relevant to a local authority, are directed covert surveillance in respect of specific operations involving criminal offences that are either punishable by a maximum term of at least 6 months' imprisonment or are related to the underage sale of tobacco or alcohol, and the use of covert human intelligence sources (see Guidance – Part 2 below). The Act makes it clear for which purposes they may be used, to what extent, and who may authorise their use. There are also Codes of Practice in relation to the use of these powers and the Home Office web site links for these is at **Appendix C.**

2.3 Consideration must be given, prior to authorisation as to whether or not the acquisition of private information is necessary and proportionate, i.e. whether a potential breach of a human right is justified in the interests of the community as a whole, or whether the information could be gleaned in other ways.

3. **Scrutiny and Tribunal**

As from 1 November 2012 councils have had to obtain an order from a Justice of the Peace approving the grant or renewal of any authorisation for the use of directed surveillance or CHIS before the authorization can take effect and the activity carried out. The Council can only appeal a decision of the Justice of the Peace on a point of law by judicial review.

The Office of Surveillance Commissioners (OSC) was set up to monitor compliance with RIPA. The OSC has "a duty to keep under review the exercise and performance by the relevant persons of the powers and duties under Part II of RIPA", and the Surveillance Commissioner will from time to time inspect the Council's records and procedures for this purpose.

In order to ensure that investigating authorities are using the powers properly, the Act also establishes a Tribunal to hear complaints from persons aggrieved by conduct, e.g. directed surveillance. Applications will be heard on a judicial review basis.
Such claims must be brought no later than one year after the taking place of the conduct to which it relates, unless it is just and equitable to extend this period.

The Tribunal can order:

- Quashing or cancellation of any warrant or authorisation
- Destruction of any records or information obtained by using a warrant or Authorisation
- Destruction of records or information held by a public authority in relation to any person

The Council has a duty to disclose to the tribunal all documents they require if any Council officer has:

- Granted any authorisation under RIPA
- Engaged in any conduct as a result of such authorisation.

4. **Benefits of RIPA authorisations**

The Act states that if authorisation confers entitlement to engage in a certain conduct and the conduct is in accordance with the authorisation, then it will be lawful for all purposes. Consequently, RIPA provides a statutory framework under which covert surveillance can be authorised and conducted compatibly with Article 8 of the Human Rights Act 1998 – a person's right to respect for their private and family life, home and correspondence.

Material obtained through properly authorised covert surveillance is admissible evidence in criminal proceedings.

5. **Definitions**

5.1 'Covert' is defined as surveillance carried out in such a manner that is calculated to ensure that the person subject to it is unaware that it is or may be taking place. (s.26 (9)(a))

5.2 'Directed surveillance' is defined as covert but not intrusive and undertaken:

- for a specific investigation or operations,
- in such a way that is likely to result in the obtaining of private information about any person
- other than by way of an immediate response (s.26 (2))

5.3 'Private information' includes information relating to a person's private or family life.

5.4 'Intrusive' surveillance is 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 using a surveillance device. **Rushcliffe Borough Council may not authorise such surveillance, nor the entry on or interference with property or with wireless telegraphy.**

5.5 'Authorising officer' - in the case of local authorities these are specified as Director, Head of Service, Service Manager and more senior officers (see Regulation of Investigatory Powers (Directed Surveillance and Covert Human Intelligence Sources) Order 2010 (SI 2010 No.521)). A list of Rushcliffe's designated authorising officers is attached as **Appendix D.**

6. When does RIPA apply?

The Council can only authorise directed surveillance to prevent and detect conduct which constitutes one or more criminal offences. The criminal offences must be punishable, whether on summary conviction or indictment by a maximum term of at least 6 months imprisonment or be an offence under:

a) Section 146 of the Licensing Act 2003 (sale of alcohol to children)
b) Section 147 of the Licensing Act 2003 (allowing the sale of alcohol to children)
c) Section 147A of the Licensing Act 2003 (persistently selling alcohol to children)
d) Section 7 of the Children and Young Persons Act 1933 (sale of tobacco etc to persons under 18.

CCTV

The normal use of CCTV is not usually covert because members of the public are informed by signs that such equipment is in operation. However, authorisation should be sought where it is intended to use CCTV covertly, and in a pre-planned manner as part of a specific investigation or operation, to target a specific individual or group of individuals. Equally a request, say by the police, to track particular individuals via CCTV recordings may require authorisation (from the police). See too OSC Procedures and Guidance 2014, paragraphs 271-272.

SOCIAL NETWORKING SITES

The fact the digital investigations are routine, easy to conduct or apparently public does not reduce the need for authorisation. Any surveillance carried out on the internet must be carried out in accordance with this policy if the criteria are met.

Guidance issued by the Office of Surveillance Commissioners in connection with the use of Social Media offers the following:

"Authorising Officers must not be tempted to assume that one service provider is the same as another or that the services provided by a single provider are the same.

Whilst it is the responsibility of an individual to set privacy settings to protect unsolicited access to private information, and even though 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. In some cases data may be deemed private communication still in transmission (instant messages for example). Where privacy settings are available but not applied the data may be considered open source and an authorisation is not usually required. Repeat viewing of "open source" sites may constitute directed surveillance on a case by case basis and this should be borne in mind.

Providing there is no warrant authorising interception in accordance with section 48(4) of the 2000 Act, if it is necessary and proportionate for a public authority to breach covertly access controls, the minimum requirement is an authorisation for directed surveillance. An authorisation for the use and conduct of a CHIS is necessary if a relationship is established or maintained by a member of a public authority or by a person acting on its behalf (i.e. the activity is more than mere reading of the site's content).

It is not unlawful for a member of a public authority to set up a false identity but it is inadvisable for a member of a public authority to do so for a covert purpose without authorisation. Using photographs of other persons without their permission to support the false identity infringes other laws.

A member of a public authority should not adopt the identity of a person known, or likely to be known, to the subject of interest or users of the site without authorisation, and without the consent of the person whose identity is used, and without considering the protection of that person. The consent must be explicit (i.e. the person from whom consent is sought must agree (preferably in writing) what is and is not to be done)."

7. Authorisations

7.1 Applications for directed surveillance

7.1.1 All application forms (**see Appendix B**) must be fully completed with the required details to enable the authorising officer to make an informed decision.

No authorisation shall be granted unless the authorising officer is satisfied that the investigation is:

- necessary for one of the purposes listed above (see paragraph 6).
- proportionate to the ultimate objective
- at an appropriate level (i.e. not excessive)

and that no other form of investigation would be appropriate.

The grant of authorisation should indicate that consideration has been given to the above points.

Necessity: Covert surveillance cannot be said to be necessary if the desired information can reasonably be obtained by overt means. It must also be necessary by reference to one or more of the statutory grounds.

Proportionality: The method of surveillance proposed must not be excessive in relation to the seriousness of the matter under investigation. It must be the method which is the least invasive of the target's privacy. Detailed advice is set out in the OSC Procedures and Guidance (Dec 2014), paragraphs 73 -74).

7.1.2 The authorising officer must also take into account the risk of **'collateral intrusion'** i.e. intrusion on, or interference with, the privacy of persons other than the subject of the investigation. The application must include an **assessment** of any risk of collateral intrusion for this purpose.

Steps must be taken to avoid unnecessary collateral intrusion and minimise any necessary intrusion.

Those carrying out the investigation must inform the authorising officer of any unexpected interference with the privacy of individuals who are not covered by the authorisation, as soon as these become apparent. When such collateral intrusion is unavoidable, the activities may still be authorised provided this intrusion is considered proportionate to what is sought to be achieved.

Further guidance on Collateral Intrusion can be found in paragraphs 3.8-3.11 of the Code of Practice on Covert Surveillance and Property Interference (2010 Rev).

7.1.3 **Special consideration in respect of confidential information**

Particular attention is drawn to areas where the subject of surveillance may reasonably expect a high degree of privacy, e.g. where confidential information is involved.

Confidential information consists of matters subject to legal privilege, communications between a Member of Parliament and another person on constituency matters, confidential personal information or confidential journalistic material. (ss 98-100 Police Act 1997).

Legal privilege

Generally, this applies to communications between an individual and his/her legal adviser in connection with the giving of legal advice in connection with or in contemplation of legal proceedings. Such information is unlikely ever to be admissable as evidence in criminal proceedings.

If in doubt, the advice of the Council's Solicitor should be sought in respect of any issues in this area.

Confidential personal information

This is oral or written information held in (express or implied) confidence, relating to the physical or mental health or spiritual counseling concerning an individual (alive or dead) who can be identified from it. Specific examples provided in the codes of practice are consultations between a health professional and a patient, discussions between a minister of religion and an individual relating to the latter's **spiritual welfare** or matters of **medical or journalistic confidentiality**.

Confidential journalistic material

This is material acquired or created for the purposes of journalism and held subject to an undertaking to hold it in confidence.

It should be noted that matters considered to be confidential under RIPA may not necessarily be properly regarded as confidential under section 41 Freedom of Information Act.

Where such information is likely to be acquired, the surveillance may only be authorised by the Chief Executive, or, in his absence, a Chief Officer and should only be authorised where there are exceptional and compelling circumstances that make the authorisation necessary.

7.1.3 Authorisations must be in writing except in urgent cases but these should be followed up in writing as soon as possible. Urgency only arises where to await written authorisation would endanger life or jeopardise the operation. Delay caused in obtaining an authorisation cannot justify an urgent, oral authorisation.

In urgent cases the authorising officer and the applicant should also record the following information in writing, as soon as is reasonably practicable:

- The identities of those subject to surveillance
- The nature of the surveillance
- The reasons why the authorising officer considered the case so urgent as to justify an oral application

8.1.5 Judicial Approval of authorisations

Once the authorising officer has authorised the Directed Surveillance or CHIS, the Investigating Officer who completed the application form should contact the Magistrates Court to arrange a hearing for the authorisation to be approved by a Justice of the Peace.

The Investigating Officer will provide the Justice of the Peace with a copy of the original authorisation 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.

In addition the Investigator will provide the Justice of the Peace with a partially completed judicial application/order form.

The hearing will be in private and the officer will be sworn in and present evidence as required by the Justice of the Peace. Any such evidence should be limited to the information in the authorisation.

The Justice of the Peace will consider whether he/she is satisfied that at the time the authorisation was given there were reasonable grounds for believing that the authorisation or notice was necessary and proportionate and whether that continues to be the case. They will also consider whether the authorisation was given by the appropriate designated person at the correct level within the Council and whether (in the case of directed surveillance) the crime threshold has been met.

The Justice of the Peace can :

a) **Approve the grant of the authorisation** ,which means the authorisation will then take effect.
b) **Refuse to approve the grant of the authorisation**, which means the authorisation will not take effect but the Council could look at the reasons for refusal, make any amendments and reapply for judicial approval.

c) **Refuse to approve the grant of the authorisation** and quash the original authorisation. The court cannot exercise its power to quash the authorisation unless the applicant has at least 2 business days from the date of the refusal in which to make representations

8.1.6 **Notifications to Inspector/Commissioner**

The following situations must be brought to the inspector/commissioner's attention at the next inspection:

- Where an officer has had to authorise surveillance in respect of an investigation in which he/she is directly involved.
- Where a lawyer is the subject of an investigation or operation;
- Where confidential personal information or confidential journalistic information has been acquired and retained.

.

8. **Duration and Cancellation**

- An authorisation for **directed surveillance** shall cease to have effect (if not renewed) 3 months from the date the Justice of the Peace approves the grant or renewal.
- If renewed the authorisation shall cease to have effect 3 months from the expiry of the original authorisation.

- An **oral** authorisation or renewal shall cease to have effect (unless renewed) 72 hours from the date of grant or renewal.

This does not mean that the authorisation should continue for the whole period so that it lapses at the end of this time. The applicant must apply to cancel each authorisation as soon as that officer decides that the surveillance should be discontinued.

When cancelling an authorisation, the authorising officer must ensure that proper arrangements have been made for the activity's discontinuance, including the removal of technical equipment and directions for the management of the product (see too 12. below).

9. **Reviews**

The authorising officer should review all authorisations at intervals determined by him/herself. This should be as often as necessary and practicable. The reviews should be recorded.

Particular attention should be paid to the possibility of obtaining confidential information.

10. **Renewals**

Any authorising officer may renew an existing authorisation on the same terms as the original at any time before the original ceases to have effect. The renewal must then be approved by the Justice of the Peace in the same way the original authorisation was approved.

11. **Records of authorisations**

11.1 All authorities must maintain the following documents:

- Copy of the application and a copy of the authorisation together with any supplementary documentation and notification of the approval given by the authorised officer;
- Copy of the Order made by the magistrates' court
- A record of the period over which the surveillance has taken place;
- The frequency of reviews prescribed by the authorising officer;
- A record of the result of each review of the authorisation;
- A copy of any renewal of an authorisation and Order made by the magistrates' court and supporting documentation submitted when the renewal was requested;
- The date and time when any instruction to cease surveillance was given by the authorising officer.
- The date and time when any other instruction was given by the authorising officer

11.2 The original copy of every authorisation, review, renewal and cancellation issued should be lodged immediately with the Solicitor to the Council in an envelope marked 'Private and Confidential'. Any original authorisations and renewals taken to the magistrates' court should be retained by the Council and the Court should retain only *copies* of the authorisations or renewals.

11.3 The Council must also maintain a centrally retrievable record of the following information (the Central Register):

- type of authorisation
- date the authorisation was given
- date the approval order was given by the Justice of the Peace
- name and rank/grade of the authorising officer and whether 'self-authorised'
- unique reference number of the investigation/operation
- title (including brief description and names of the subjects) of the investigation/operation;
- whether urgency provisions were used and if so why
- details of renewal
- dates of any approval order for renewal given by the Justice of the Peace
- whether the investigation/operation is likely to result in obtaining confidential information
- date of cancellation

These records will be retained by the Solicitor to the Council for at least 3 years and will be available for inspection by the Office of Surveillance Commissioners.

12. **Retention of records**

12.1 All documents must be treated as strictly confidential and the authorising officer must make appropriate arrangements for their retention, security and destruction, in accordance with the Council's Data Protection Policy and the RIPA codes of practice. The recommended retention period for authorisation records is three years from the ending of the period authorised.

12.2 Appropriate arrangements must be put in place for the handling, storage and destruction of material obtained through the use of covert surveillance ("the product"). Authorising officers must ensure compliance with the relevant data protection requirements and any relevant codes of practice.

13. **Complaints procedure**

13.1 The Council will maintain the standards set out in this guidance and the Codes of Practice (**See Appendix C**). The Chief Surveillance Commissioner has responsibility for monitoring and reviewing the way the Council exercises the powers and duties conferred by RIPA.

13.2 Contravention of the Data Protection Act 1998 may be reported to the Information Commissioner. Before making such a reference, a complaint concerning a breach of this guidance should be made using the Council's own internal complaints procedure. To request a complaints form, please contact the Performance and Reputation Team, Rushcliffe Borough Council, Civic Centre, Pavilion Road, West Bridgford, Nottingham, NG2 5FE or telephone Customer Services on 0115 981 9911

REGULATION OF INVESTIGATORY POWERS ACT 2000 (RIPA)

GUIDANCE – PART 2

COVERT HUMAN INTELLIGENCE SOURCES

Covert Human Intelligence Source

The RIPA definition (section 26(8)) is anyone who:

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

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

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

Any reference to the conduct of a CHIS includes the conduct of a source which falls within a) to c) or is incidental to it.

References to the use of a CHIS are references to inducing, asking or assisting a person to engage in such conduct.

Section 26(9) of RIPA goes on to define:-

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

(c) a relationship is used covertly, and information obtained as mentioned in ss (8) (c) above and is disclosed covertly, if, and only if it is used or as the case may be, disclosed in a manner that is calculated to ensure that one of the parties to the relationship is unaware of the use or disclosure in question.

There is a risk that an informant who is providing information to the Council voluntarily may in reality be a CHIS even if not tasked to obtain information covertly. It is the activity of the CHIS in exploiting a relationship for a covert purpose which is ultimately authorised in the 2000 Act, not whether or not the CHIS is asked to do so by the Council. When an informant gives repeat information about a suspect or about a family and it becomes apparent that the informant may be obtaining the information in the course of a neighbourhood or family relationship, it may mean that the informant is in fact a CHIS. Legal advice should always be sought in such instances before acting on any information from such an informant.

Attention is also drawn to the advice at paragraph 6 above concerning the use of social networking sites.

Applications for CHIS

NB. The Borough Council is unlikely to need to use CHIS **and the Council's Solicitor should be consulted before any authorisation is sought.**

The procedure is the same as for directed surveillance except that the authorisation must specify the activities and identity of the CHIS and that the authorised conduct is carried out for the purposes of, or in connection with, the investigation or operation so specified.

All application forms **(see Appendix B)** must be fully completed with the required details to enable the authorising officer to make an informed decision.

An authorisation for CHIS shall cease to have effect (unless renewed) 12 months from the date of grant or renewal. A CHIS authorisation must be thoroughly reviewed before it is renewed.

REGULATION OF INVESTIGATORY POWERS ACT 2000

GUIDANCE – PART 3

ACQUISITION AND DISCLOSURE OF COMMUNICATIONS DATA

Introduction

With effect from 5 January 2004, and in accordance with Chapter II of Part I of Regulation of Investigatory Powers Act ("the Act"), local authorities can authorise the acquisition and disclosure of 'communications data' provided that the acquisition of such data is necessary for the purpose of preventing or detecting crime or preventing disorder; and proportionate to what is sought to be achieved by acquiring such data.

There is a Code of Practice (see **Appendix C**) ("the Code")

NOTHING IN THIS CODE PERMITS THE INTERCEPTION OF THE CONTENT OF ANY COMMUNICATION.

The procedure is similar to that of authorisation for directed surveillance and CHIS but has extra provisions and processes.

The purpose and effect of the procedure is the same i.e. to ensure proper consideration is given to permitting such investigations and to provide protection against a human rights challenge. **All potential applications shall be referred initially to the Solicitor to the Council for advice.**

The authorising officer is called a 'designated person'.

1. **What is 'Communications data'?**

   Communications data is information relating to the use of a communications service e.g. postal service or telecommunications system. It is defined by Section 21(4) of the Act and falls into three main categories:-

   Traffic data – where a communication was made from, to whom and when

   Service data – use made of service e.g. itemised telephone records

   Subscriber data – information held or obtained by operator on person they provide a service to.

   Local authorities are restricted to subscriber and service use data and only for the purpose of preventing or detecting crime or preventing disorder.

2. **Designated person**

A designated person must be at least the level of Assistant Chief Officer, Assistant Head of Service, Service Manager or equivalent.

3. **Application forms**

All applications must be made on a standard form (see **Appendix B).**

4. **Authorisations**

Authorisations can only authorise conduct to which Chapter II or Part I of the Act applies.

In order to comply with the code, a designated person can only authorise the obtaining and disclosure of communications data if:

i) It is **necessary** for any of the purposes set out in Section 22(2) of the Act. (NB. Rushcliffe Borough Council can only authorise for the purpose set out in Section 22(2)(b) which is the purpose of preventing or detecting crime or preventing disorder); and

ii) It is **proportionate** to what is sought to be achieved by the acquisition of such data (in accordance with Section 22(5) the Act)

Consideration must also be given to the possibility of collateral intrusion and whether any urgent timescale is justified.

Once a designated person has decided to grant an authorisation or a notice given there are two methods:-

1) By authorisation of some person in the same relevant public authority as the designated person, whereby the relevant public authority collects the data itself (Section 22(3) the Act). This may be appropriate in the following circumstances:

- The postal or telecommunications operator is not capable of collecting or retrieving the communications data.
- It is believed the investigation may be prejudiced if the postal or telecommunications operator is asked to collect the data itself;
- There is a prior agreement in place between the relevant public authority and the postal or telecommunications operator as to the appropriate mechanisms for the disclosure of communications data.

2) By notice to the holder of the data to be acquired (Section 22(4)) which requires the operator to collect or retrieve the data. Disclosure may only be required to either the designated person or the single point of contact.

Service provider must comply with the notice if it is reasonably practicable to do so (s.22(6)-(8)) and can be enforced to do so by civil proceedings.

The postal or telecommunications service can charge for providing this information.

There are standard forms (see **Appendix B**) for authorisations and notice.

5. Oral authority

The Council is not permitted to apply or approve orally.

6. Single point of contact (SPOC)

Notices and authorisations should be passed through a single point of contact within the Council. This should make the system operate more efficiently as the SPOC will deal with the postal or telecommunications operator on a regular basis and also be in a position to advise a designated person on the appropriateness of an authorisation or notice.

SPOCs should be in position to:

- Where appropriate, assess whether access to communication data is reasonably practical for the postal or telecommunications operator;
- Advise applicants and designated person on whether communications data falls under Section 21(4)(a), (b) or (c) of the Act;
- Provide safeguards for authentication;
- Assess any cost and resource implications to both the public authority and the postal or telecommunications operator.

7. Duration

Authorisations and notices are only valid for one month beginning with the date on which the authorisation is granted or the notice given. A shorter period should be specified if possible.

8. Renewal and cancellation

An authorisation or notice may be renewed at any time during the month it is valid using the same procedure as used in the original application. A renewal takes effect on the date which the authorisation or notice it is renewing expires.

The code requires that all authorisations and notices should be cancelled by the designated person who issued it as soon as it is no longer necessary, or the conduct is no longer proportionate to what is sought to be achieved. The

relevant postal or telecommunications operator should be informed of the cancellation of a notice.

9. **Retention of records**

Applications, authorisations and notices must be retained until the Council has been audited by the Commissioner (see paragraph 10).

Applications must also be retained to allow the Tribunal (see paragraph 10) to carry out its functions.

A record must be kept of:-

- the dates on which the authorisation or notice is started or cancelled.
- any errors that have occurred in the granting of authorisations or giving of notices.

A report and explanation of any errors must also be sent to the Commissioner as soon as is practicable.

Communications data, and all copies, extracts and summaries of it, must be handled and stored securely and the requirements of the Data Protection Act 1998 must be observed.

10. **Oversight and Complaints**

The Act provides for an Interception of Communications Commissioner whose remit is to provide independent oversight of the use of the powers contained in Part I and the code requires any person who uses the powers conferred by Chapter II to comply with any request made by the Commissioner to provide any information he requires to enable him to discharge his functions.

The Act also establishes an independent Tribunal to investigate and decide any case within its jurisdiction. Details of the relevant complaints procedure should be available for reference at Rushcliffe Borough Council's public offices.

APPENDIX A

SCRUTINY ARRANGEMENTS

The following arrangements have been put in place to comply with the requirements set out in the revised Codes of Practice published by the Home Office in 2010.

Senior Responsible Officer

The SRO shall be responsible for -

- the integrity of the process in place to authorise directed surveillance and CHIS
- compliance with Part II of the 2000 Act and with the accompanying Codes of Practice
- engagement with the Surveillance Commissioners and Inspectors when they conduct their inspections, and
- where necessary, oversight of the implementation of any post-inspection action plans recommended or approved by a Commissioner.

The SRO is the Monitoring Officer and a member of the Council's Corporate Management Team. He is responsible for ensuring that all authorising officers are suitably qualified and trained.

Elected Member Involvement

The SRO will report annually to the relevant Cabinet portfolio holder with the following information -

- the current Policy and Guidance being used by the Council
- statistics and overview of the use of directed surveillance and CHIS by the Council during the previous year
- following an OSC inspection, detailing any recommendations made and the action(s) taken in response to those recommendations

Any significant issues arising shall also be reported to a meeting of Cabinet.

APPENDIX B

Forms

See Home Office website:

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

APPENDIX C

Codes of Practice

See Home Office website:

http://www.homeoffice.gov.uk/counter-terrorism/regulation-investigatory-powers/ripa-codes-of-practice/

APPENDIX D

RUSHCLIFFE BOROUGH COUNCIL

Senior Responsible Officer and Authorised Officers

RIPA Coordinator

The designated Senior Responsible Officer for the RUSHCLIFFE BOROUGH COUNCIL under the Regulation of Investigatory Powers Act 2000 shall be:

Officer	Department	Contact details
Mr Phil Horsfield	Monitoring Officer Civic Centre, Pavilion Road, West Bridgford, Nottingham, NG2 5FE	Tel: 0115 914 8349 E-mail: phorsfield@rushcliffe.gov.uk

Authorising Officers

The following officers shall be designated as Authorising Officers for the specified purpose on behalf of RUSHCLIFFE BOROUGH COUNCIL under the Regulation of Investigatory Powers Act 2000:

Name	Post
Mr A Graham	Chief Executive
Mr D Banks	Executive Manager Neighbourhoods
Mr B Adams	Environment and Licensing Manager

June 2016