

RUSHCLIFFE BOROUGH COUNCIL

REGULATION OF INVESTIGATORY POWERS

ACT 2000 (RIPA)

POLICY AND GUIDANCE

Contents

Policy on Regulation of Investigatory Powers Act 2000 (RIPA)	Page 2
Part 1 – Directed Surveillance	Page 4
Part 2 – Covert Human Intelligence Sources (CHIS)	Page 18
Part 3 – Acquisition and Disclosure of Communications Data	Page 21
Appendix A – Scrutiny Arrangements	Page 27
Appendix B – Links to Home Office - Forms	Page 29
Appendix C – Links to Home Office - Codes of Practice	Page 30
Appendix D – List of RBC Authorising Officers	Page 31

RUSHCLIFFE BOROUGH COUNCIL

POLICY ON REGULATION OF INVESTIGATORY POWERS ACT 2000 (RIPA)

1. Introduction

- 1.1 The Regulation of Investigatory Powers Act 2002 (as amended) (“RIPA” or “the Act”) came into force on 24th September 2000 and aims to balance, in accordance with the European Convention of Human Rights, the rights of individuals with the need for law enforcement and security agencies to have powers to perform their roles effectively. The Act and amending legislation allow local authorities to collect evidence of criminal activity lawfully where the investigation requires covert surveillance even where that may lead to them obtaining private information about individuals.
- 1.2 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 this Guidance document to assist officers.
- 1.3 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, the Data Protection Act 2018 and its common law obligations.

2. Applications for authority

- 2.1 Where an investigating officer identifies a contemplated surveillance activity as being regulated by RIPA, written authorisation in accordance with this Policy must be obtained before commencement of the activity. An officer authorised by the Council (see definition of Authorising Officer below) 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 for the prevention and

detection of crime or preventing disorder;

- proper consideration has been given to collateral intrusion;
- the proposed length and extent of the surveillance is proportionate to the information being sought;
- the 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 Monitoring Officer for entry on the Central Register; and
- 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

If enforcement officers or their managers are in any doubt, they should contact the Legal Services department for advice.

3. Training

- 3.1 Each Head of Service 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 as necessary.

4. Central register and records

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

5. Scrutiny

- 5.1 The Council has appointed the Monitoring Officer as the Senior Responsible Officer ("SRO").
- 5.2 Further detail of the role of the SRO and the role of elected members is set out in Appendix A.

POWERS ACT 2000 (RIPA)

PART I Directed Surveillance**6. Purpose**

- 6.1 The purpose of this is to explain the scope of RIPA, the circumstances where it applies and the authorisations procedures to be followed.

7. Introduction

- 7.1 The Act 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 the Human Rights Act 1998. This is achieved by requiring certain investigations to be authorised by an appropriate officer and approved by the judiciary before they are carried out.
- 7.2 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, whether on summary conviction or indictment, by a maximum term of at least 6 months' imprisonment or are related to the underage sale of alcohol and tobacco, and the use of covert human intelligence sources ("CHIS"). 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 these are attached at Appendix C.
- 7.3 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.

8. Scrutiny and Tribunal

- 8.1 As of 1 November 2012, councils have to obtain an order from a Magistrate approving the grant or renewal of any authorisation for the use of directed surveillance or CHIS before the authorisation can take effect and the activity carried out. The Council can only appeal a decision of the Magistrate on a point of law by judicial review.
- 8.2 The Investigatory Powers Commissioner (IPC), a role established by the Investigatory Powers Act 2016, has comprehensive oversight of the use of RIPA powers by public authorities and will ensure compliance with the law by inspecting public authorities and investigating any issue which they believe warrants further scrutiny. The IPC will have unfettered access to all locations,

documentation and information systems necessary to carry out their full functions and duties.

- 8.3 In order to ensure that investigating authorities are using the powers properly, the Act also establishes the Investigatory Powers Tribunal (IPT) 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. Further information about the IPT can be found at www.ipt-uk.com.
- 8.4 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
- 8.5 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.
- 8.6 Internal scrutiny
- 8.6.1 The Council will ensure that the SRO is responsible for;
- The integrity of the process in place within the Council to authorise directed surveillance and CHIS
 - Compliance with PART II of the 2000 Act and with the accompanying Codes of Practice
 - Engagement with the Commissioner and inspectors when they conduct their inspections and
 - Where necessary overseeing the implementation of any post-inspection action plans recommended or approved by the Commissioner
- 8.6.2 The elected members of the Council will review the Council's use of the Act and the Council's policy and guidance documents at least once a year. Members will also consider internal reports on a regular basis throughout the year indicating the nature of RIPA activity undertaken or inactivity, to ensure that any use is consistent with the Council's policy and that the policy is fit for purpose. The members will not

however be involved in making decisions on specific authorisations.

8.7 Unauthorised Activities

- 8.7.1 If any Officer is concerned that surveillance/CHIS activity is taking place and there is no authorisation under RIPA in place, he/she should be contacted by Legal Services to seek advice.
- 8.7.2 If any activity is deemed to be unauthorised, it will be reported to the IPC.

9. Benefits of RIPA authorisations

- 9.1 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.
- 9.2 Material obtained through properly authorised covert surveillance is admissible evidence in criminal proceedings, as long as it complies with the provisions of RIPA.
- 9.3 Compliance with RIPA ensures any interference is carried out in accordance with domestic laws. It also assists to defend any complaints against the Council and its officers of interference with the right to respect for private and family life which is protected by Article 8. The Council can claim the interference is 'in accordance with the law'. The activities undertaken however must be necessary and proportionate.

10. Definitions

'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))

'Covert human intelligence source' (CHIS) is defined as a person who establishes or maintains a personal or other relationship with a person for the covert process of obtaining/providing access to/disclosing, information obtained through that relationship or as a consequence of the relationship (s.26 (8))

'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, and

- other than by way of an immediate response (s.26 (2))

'Private information' includes information relating to a person's private or family life (s.26(10)). Private information should be taken generally to include information on any aspect of a person's private or personal relationship with others including family and professional or business relationships. It is likely to be the case that where a person has a reasonable expectation of privacy, even though acting in public or placing information on publicly accessible areas of the internet, and where a record of that activity is being made by a public authority of that person's activities for future consideration or analysis, that this will result in obtaining private information.

'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.**

'Authorising officer' - in the case of the Council a list of designated authorising officers can be found at **Appendix D.**

11. When does RIPA apply?

- 11.1 The Council can only authorise directed surveillance of an individual or group of individuals, or use of CHIS where it is **necessary** for the purpose of preventing or detecting crime or preventing disorder.
- 11.2 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)

12. Core Functions

- 12.1 A public authority may only seek authorisations under the Act when in performance of its 'core functions'. Core functions are the specific public functions undertaken by the authority in contrast to the ordinary functions which are those undertaken by all authorities, for example, employment issues or contractual arrangements. The disciplining of an employee is not a core function, although related criminal investigations may be.

13. CCTV

- 13.1 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). Guidance on the operation of CCTV generally is provided in the Surveillance Camera Code of Practice (as amended) issued under the Protection of Freedoms Act 2012. The Information Commissioner has also issued a code 'In the Picture – A Data Protection Code of Practice for Surveillance Cameras and Personal Information' which authorities should have regard to.

14. Online Covert Activity

- 14.1 The use of the internet and social media sites may be required to gather information prior to and during an operation/investigation. Officers should exercise caution when utilising such sites during an investigation and be alert to situations where authorisations under RIPA may be required. If officers have any concerns over the use of social media during an investigation they should contact Legal Services. As a general rule of thumb however, reviewing open source sites such as Facebook pages where no privacy settings are in place does not require an authorisation under RIPA unless review is carried out with some regularity, often to build a profile, when directed surveillance authorisation may be required.
- 14.2 Use of the internet prior to an investigation should not normally engage privacy considerations but if the study of an individual's online presence becomes persistent, or where material obtained from any check is to be extracted and recorded and may engage privacy considerations, a RIPA authorisation may be required. If the officer then, for the purposes of gleaning intelligence breaches privacy controls and becomes for example a "friend" within a subject's Facebook account, utilising a pseudo account to conceal his/her identity as a Council official, this is a covert operation which, by its nature, is intended to obtain private information and should be authorised as a minimum as directed surveillance. Further, if the officer engages in any form of relationship with the

account operator then s/he is likely to become a CHIS requiring authorisation and management by a Controller and Handler with a record being kept and a risk assessment created.

- 14.3 In deciding whether online surveillance should be regarded as covert, consideration should be given to the likelihood of the subject knowing that surveillance is or may be taking place. This is regardless of what privacy settings the individual may have in place.

15. Authorisations

- 15.1 **Applications for directed surveillance** All application forms must be fully completed with the required details to enable the authorising officer to make an informed decision.
- 15.2 Application forms are available on the Home Office website, officers should ensure they are using the most up to date forms for RIPA authorisations. The authorisation will only commence on the date Magistrates Court approval is obtained and runs for three months from that date of that approval
- 15.3 No authorisation shall be granted unless the authorising officer is satisfied that the investigation is:
- necessary - for either the purpose of preventing or detecting crime or of preventing disorder. Covert surveillance cannot be said to be necessary if the desired information can reasonably be obtained by overt means
 - Involves a criminal offence punishable whether summarily or on indictment by a maximum sentence of at least six months imprisonment or related to the underage sale of alcohol or tobacco
 - proportionate to the ultimate objective at an appropriate level (not excessive) and that no other form of investigation would be appropriate. This has 4 elements, namely:
 - (1) that the method of surveillance proposed is not excessive to the seriousness of the matter under investigation,
 - (2) the method used must be the least invasive of the target's privacy,
 - (3) the privacy of innocent members of the public must be respected and collateral intrusion minimised.
 - (4) that no other form of investigation would be appropriate. This should be evidenced by explaining what other methods of investigation have been considered or tried and why they have not been implemented or why they failed.

- 15.4 The grant of authorisation should indicate that consideration has been given to the above points.
- 15.5 The authorising officer must also take into account the risk of **'collateral intrusion'**, for example, 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.
- 15.6 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. The same considerations in respect of proportionality outlined above apply to the assessment of collateral intrusion.
- 15.7 The Authorising Officer should also fully understand the capabilities and sensitivity levels of any equipment being used to carry out directed surveillance so as to properly assess the risk of collateral intrusion in surveillance techniques.

16. Special consideration in respect of confidential information

- 16.1 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.
- 16.2 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

- 16.3 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 admissible as evidence in criminal proceedings.
- 16.4 If in doubt, the advice of the Monitoring Officer should be sought in respect of any issues in this area.

Confidential personal information

16.5 This is oral or written information held in (express or implied) confidence, relating to the physical or mental health or spiritual counselling 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 constituent information

16.6 This is information relating to communication between a Member of Parliament and a constituent in respect of constituency business. Such information is held in confidence if it is held subject to an express or implied undertaking to hold it in confidence or it is subject to a restriction on disclosure or an obligation of confidentiality contained in existing legislation.

Confidential journalistic material

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

16.8 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 their absence, a Chief Officer and should only be authorised where there are exceptional and compelling circumstances that make the authorisation necessary.

Authorisations must be in writing and have a wet signature

16.9 Authorising officers are not responsible for authorising investigations or operations in which they have been directly involved. Whilst it has been recognised that this may sometimes be unavoidable in cases where it is necessary to act urgently the authorising officer authorises such an investigation or operation should place a note of the authorisation on the central record of authorisation.

16.10 Authorising officers must be aware of the requirements of RIPA and how to properly consider requests for authority. The authorising officer must demonstrate that the request has been properly considered when completing the application.

17 Applications for CHIS

- 17.1 The process for CHIS applications is the same as for Directed Surveillance except that the serious crime threshold of investigating criminal offences with a sentence of at least 6 months in imprisonment does not apply. The authorisation must be in writing, must specify the activities and identity (by pseudonym only) 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.
- 17.2 Again the Authorising Officer must be satisfied that the authorised use and conduct of the CHIS is proportionate to what is sought to be achieved by that conduct and the CHIS must be necessary for the prevention or detection of crime or the prevention of disorder. Collateral intrusion must also be considered.
- 17.3 All application forms must be fully completed with the required details to enable the Authorising Officer to make an informed decision. A risk assessment and record must be prepared for each CHIS.

18 Judicial Approval of authorisations

- 18.1 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 Authorising Officer should make themselves available to attend court with the Investigating Officer. The hearing should ideally be on the same day as the Authorising Officer gives authorisation, the court should be contacted prior to attendance to ensure the matter can be heard.
- 18.2 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 and should contain all information that is relied upon.
- 18.3 The Investigating Officer will provide the Magistrate with a partially completed judicial application/order form. These documents should be taken to the court by the Investigating Officer and not sent to the court by any other means prior to the hearing. Officers may seek support from Legal Services in completing the application/order form.
- 18.4 The hearing will be in private and the Investigating 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.

18.5 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.

18.6 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

19 Notifications to Inspector/Commissioner

19.1 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.

20 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 renewed 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 Authorising Officer must cancel the authorisation at any time if they consider that the Directed Surveillance no longer meets the criteria upon which it was authorised. Where the original Authorising Officer is no longer available, this duty will fall on the person who has taken over the role of Authorising Officer or the person who is acting as Authorising Officer

20.1 On cancellation, the cancellation form should detail what product has been obtained as a result of the surveillance activity. The forms should include the dates and times of the activity, the nature of the product obtained and its format, any associated log or reference numbers, details of where the product is to be held and the name of the officer responsible for its future management. Documentation of any instruction to cease surveillance should be retained and kept with the cancellation form.

20.2 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.

21 Reviews

21.1 The Authorising Officer should review all authorisations at reasonable intervals determined by themselves. This should be as often as necessary and practicable. The reviews should be recorded within the record of authorisation.

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

22 Renewals

22.1 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 a Justice of the Peace in the same way that the original authorisation was approved.

23 Records of authorisations

23.1 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

23.2 The original copy of every authorisation, review, renewal and cancellation issued should be lodged immediately with the Monitoring Officer of 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.

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

- type of authorisation
- date the authorisation was given
- details of attendance at the Magistrates' Court, the date of the attendance, the determining Justice of the Peace, the decision of the court and the time and date of the decision
- name and rank/grade of the Authorising Officer
- unique reference number of the investigation/operation
- title (including brief description and names of the subjects) of the investigation/operation

- details and dates of reviews
- whether urgency provisions were used and if so why
- details of renewal including the name and rank of the Authorising Officer
- dates of any approval order for renewal given by the Magistrates' Court
- whether the investigation/operation is likely to result in obtaining confidential information
- date of cancellation
- whether the authorisation was granted by an individual directly involved in the investigation.

These records will be retained by the Monitoring Officer for at least 5 years and will be available for inspection by the Investigatory Powers Commissioner's Office.

24 **Unique Operation Reference Number**

24.1 Each Application for Directed Surveillance and CHIS, must have a Unique Operation Reference Number. This URN will begin with either ENV (if it is granted in the Environment and Planning Department) or FIN (if it is granted in the Finance Department), followed by a sequential number, followed by 20?? being the year in which the Authority was applied for, e.g. ENV/27/2005

25 **Retention of records**

25.1 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, UK-GDPR and Data Protection Act 2018. The recommended retention period for authorisation records is five years from the ending of the period authorised.

25.2 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

26 Working in Partnership with the Police/Collaborative Working

- 26.1 Authorisation can be granted in situations where the police rather than Rushcliffe Borough Council require the surveillance to take action, as long as the behaviour complained of, meets all criteria to grant and in addition is also of concern to the Council. Authorisation cannot be granted for surveillance requested by the police for a purely police issue.
- 26.2 The Police, as an emergency service may authorise RIPA without Magistrates approval, if an urgent situation arises and RIPA authorisation would be required urgently, the Council should contact the police if surveillance is deemed to be necessary and proportionate in an urgent situation.
- 26.3 Any person granting or applying for an authorisation will also need to be aware of particular sensitivities in the local community where the surveillance is taking place and of any other similar activities being undertaken by other public authorities which could impact on the deployment of surveillance or property interference. Where an Authorising Officers considers conflicts may arise they should consult a senior officer within the police.
- 26.4 Where the Police are carrying out surveillance and request the use of the Council's cameras to do so, the police should obtain the authorisation and provide sufficient information to the Council to enable the surveillance to be undertaken in line with the authorisation.

27 Complaints procedure

- 27.1 The Council will maintain the standards set out in this guidance and the Codes of Practice (See Appendix C). The Investigatory Powers Commissioner has responsibility for monitoring and reviewing the way the Council exercises the powers and duties conferred by RIPA.
- 27.2 Contravention of RIPA may be reported to the Investigatory Powers Tribunal. 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 make a complaint, complete the online complaints form or contact the e Communications Team, Rushcliffe Borough Council, Rushcliffe Arena, Rugby Road, West Bridgford, NG2 7YG or telephone Customer Services on 0115 981 9911

REGULATION OF INVESTIGATORY POWERS ACT 2000 (RIPA)

PART 2 COVERT HUMAN INTELLIGENCE SOURCES

28 Covert Human Intelligence Source (“CHIS”)

28.1 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

28.2 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.

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

28.4 Section 26(9) of RIPA goes on to provide that:

- a. surveillance is covert, if and only if, it is carried out in a manner that is calculated to ensure that persons who are subject to the surveillance are unaware that it is or may be taking place
- 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 is obtained as mentioned 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.

28.5 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.

28.6 With any authorised use of a CHIS, the Council must ensure that arrangements are in place for the proper oversight and management of the CHIS, this includes appointing individual officers as handlers and controllers in relation to the CHIS (s.29(5)(a) and (b)). The handler should not be the Authorising Officer. Appropriate risk assessments should also be prepared in relation to the CHIS activity.

29. Juvenile Sources

29.1 Special safeguards apply to the use or conduct of juvenile sources; that is sources under the age of 18 years. On no occasion should the use or conduct of a source under the age of 16 years be authorised to give information against his parents or any person who has parental responsibility for him. The duration of a juvenile CHIS is four months. The Regulation of Investigatory Powers (Juveniles) Order 2000 contains special provisions which must be 9 adhered to in respect of juvenile sources. Any authorisation of a juvenile CHIS must be by the Chief Executive.

30. Vulnerable Individuals

30.1 A vulnerable individual is a person who by reason of mental disorder or vulnerability or other disability, age or illness is, or may be, unable to take care of himself, or unable to protect himself against significant harm or exploitation. Any individual of this description should only be authorised to act as a source in the most exceptional circumstances. Any authorisation of a vulnerable individual as a CHIS must be by the Chief Executive.

31 Applications for CHIS

The Council may only in applying the employment of CHIS for the purpose of preventing or detecting crime or preventing disorder. The Council is unlikely to need to use CHIS and the Council's Monitoring Officer should be consulted before any authorisation is sought.

31.1 The procedure is the same as for Directed Surveillance except that the serious crime threshold of investigating criminal offences with a sentence of at least 6 months in imprisonment does not apply. 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.

- 31.2 Again the Authorising Officer must be satisfied that the authorised use and conduct of the CHIS is proportionate to what is sought to be achieved by that conduct and the CHIS must be necessary for the prevention or detection of crime or the prevention of disorder. Collateral intrusion must also be considered.
- 31.3 All application forms must be fully completed with the required details to enable the Authorising Officer to make an informed decision. A controller and handler (one of whom should be a record keeper) should be identified at this stage. The source manager should ensure that a risk assessment is carried out and appended to the application.
- 31.4 Once the Authorising Officer CHIS, the Investigating Officer shall apply to the Magistrates Court for the authorisation to be approved by a Justice of the Peace as per the guidance for Directed Surveillance (paragraph 18 onwards).
- 31.5 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. The duration of authorisation for a Juvenile CHIS is 1 month.
- 31.6 The duration of a CHIS authorisation commences at the time of the Magistrates approval of it.

REGULATION OF INVESTIGATORY POWERS ACT 2000

PART 3 ACQUISITION AND DISCLOSURE OF COMMUNICATIONS DATA

32 Introduction

32.1 With effect from 5 January 2004, and in accordance with Chapter II of Part I of Regulation of Investigatory Powers Act 2000 (“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. This guidance should be read in conjunction with the relevant Code of Practice.

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

32.2 The procedure is similar to that of authorisation for Directed Surveillance and CHIS but has extra provisions and processes.

32.3 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 Monitoring Officer for advice.**

32.4 The Authorising Officer is called a ‘Designated Person’.

33 What is ‘Communications data’?

33.1 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.

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

34 Designated person

34.1 A Designated Person are the same officers as Authorising Officers set out in Appendix D.

35 Application forms

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

36 Authorisations

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

36.2 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). This involves balancing the extent of the interference with an individual's rights and freedoms against a specific benefit to the investigation or operation being undertaken by a relevant public authority in the public interest. consideration must also be given to any actual or potential infringement of the privacy and other rights of individuals who are not the subject of the investigation or operation.

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

36.4 Communication data can be acquired by two alternative methods under RIPA:

- 1) By authorisation under section 22(3) of the Act - An authorisation granted to a member of a public authority permits that person to engage in conduct relating to the acquisition and disclosure of communications data under Part I Chapter II of RIPA. This applies where the relevant public authority collects the data itself. and 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 under Section 22(4) of the Act. A notice given to a postal or telecommunications operator requires it to disclose the relevant communications data held by it to a public authority, or to obtain and disclose the data, when it is reasonably practicable for them to do so. Disclosure may only be required to either the Designated Person or the single point of contact.

36.5 A 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.

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

37 Oral authority

37.1 The Council is not permitted to apply or approve orally.

38 Single point of contact (SPOC) - National Anti-Fraud Network (NAFN)

38.1 Since September 2014, Local Authorities can only access communications data via the National Anti-Fraud Network (NAFN). 'NAFN is a not-for-profit, non-incorporated body formed by its members to provide services which support their work in the protection of the public purse. Established in 1997, NAFN was created as a centre of excellence to provide data and intelligence to its members. This includes assisting members in the provision of effective corporate and financial governance. NAFN works with its members and other stakeholders to enhance and expand its 3 range of services. It maintains all data in a secure and confidential environment conforming to Government legislation and national best practice.

38.2 The Council is a member of NAFN. We must remain a paid up member in order to make use of its single point of contact (SPoC) service in relation to communications data.

38.3 The Council is a member, primarily to make use of other services provided

by NAFN (credit referencing, DVLA checks, debtor tracing etc.) but given that Officers could now utilise the RIPA SPoC service and obtain communications data, guidance needs to be in place to govern the process.

38.4 Notices and authorisations should be passed through the NAFN as the SPOC for 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.

38.5 The accredited SPOCs at NAFN will scrutinise the applications independently. They will provide advice to applicants and designated persons ensuring the Council acts in an informed and lawful manner.

38.6 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 the 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.

39 Judicial Approval

39.1 Under sections 23A and 23B of RIPA approval must be obtained from the Magistrates Court for all local authority requests for communications data. Judicial approval must be requested once all the internal authorisation processes have been completed, including consultation with a NAFN SPoC, but before the SPoC requests the data from the CSP.

39.2 The Council is responsible for submitting the application for judicial authorisation. It is for the local authority to decide on the most appropriate representative to present their RIPA application to the magistrate. The judicial application must include relevant documentation, including the original RIPA authorisation or notice. Once the case has been heard, the magistrate will complete a judicial order outlining their decision. Should authorisation be granted, the local authority will provide the judicial order to the NAFN SPOC.

40 Duration

40.1 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.

41 Renewal and cancellation

41.1 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.

41.2 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.

42 Retention of records

42.1 Applications, authorisations renewals cancellations and notices are confidential material and must be retained until the Council has been audited by the Commissioner (see paragraph 22/10).

42.2 Applications must also be retained to allow the Tribunal (see paragraph 2/10) to carry out its functions.

42.3 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.

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

42.5 Communications data, and all copies, extracts and summaries of it, must be handled and stored securely and the requirements of the Data Protection Act 2018 and UK GDPR must be observed.

42.6 The documents referred to herein and any information contained therein should not be disclosed to any person who does not have a legitimate need to have access to the document or to the information contained within it. Authorising officers are required in ensure proper arrangements are in place within their service areas for the retention and security of the said documents.

42.7 The Monitoring Officer maintains a register of all authorisations, reviews, cancellations and renewals. Authorising officers are required to ensure that hard copies of the said documents are forwarded to the Monitoring Officer as soon as reasonably practicable for retention.

42.8 The Monitoring Officer will review the central register periodically to remove information that is more than 6 years old unless relevant court proceedings are outstanding. All documentation no longer required will be securely disposed of.

43 Oversight and Complaints

43.1 The Act provides for an Investigatory Powers Commissioner's Office 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. As the authority uses NAFN as its SPOC, NAFN as opposed to the Council will be inspected on a regular basis. It is still important that all of the relevant documents are completed properly by the Council and stored appropriately.

43.2 The Act also establishes an independent Investigatory Powers 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 2018.

44 Senior Responsible Officer

44.1 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
- Maintaining the central record of authorisations and collating the original applications/authorisations, reviews, renewals and cancellations
- Oversight of submitted RIPA documentation
- Organising a RIPA training programme; and
- Raising RIPA awareness within the Council.

44.2 The SRO is the Monitoring Officer and a member of the Council's Corporate Management Team. They are responsible for ensuring that all Authorising Officers are suitably qualified and trained.

45 Elected Member Involvement

45.1 The SRO will report annually to the Governance Scrutiny Group 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 IPCO inspection, detailing any recommendations made and the action(s) taken in response to those recommendations

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

APPENDIX B

Forms

See Home Office website: [RIPA forms](#)

APPENDIX C

Codes of Practice

[RIPA codes - GOV.UK](#)

[acquisition and disclosure of communications data code of practice](#)

APPENDIX D**RUSHCLIFFE BOROUGH COUNCIL**

Senior Responsible Officer and Authorised Officers

Senior Responsible Officer

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

Officer	Department	Contact details
Monitoring Officer	Chief Executive Department, Legal Services Rushcliffe Arena, Rugby Road, West Bridgford, Nottingham, NG2 7YG	Tel: 0115 9148 480 E-mail: monitoringofficer@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:

Post
Chief Executive
Director - Neighbourhoods
Head of Service – Public Protection

Enhanced Authorising Officer

The CHIEF EXECUTIVE shall be designated as Authorising Officers for the specified purpose on behalf of RUSHCLIFFE BOROUGH COUNCIL under the Regulation of Investigatory Powers Act 2000 when knowledge of confidential or privileged

information is likely to be acquired.