

RIBBLE VALLEY BOROUGH COUNCIL REPORT TO POLICY & FINANCE COMMITTEE

Agenda Item No.

meeting date: 7 NOVEMBER 2017
title: SURVEILLANCE COMMISSIONERS INSPECTION REPORT DATED 14 AUGUST 2017
submitted by: CHIEF EXECUTIVE
principal author: MAIR HILL

1. PURPOSE

1.1 To report to Committee the receipt of the Office of Surveillance Commissioners inspection report 14 August 2017 and to seek approval of the revised policy.

1.2 Relevance to the Council's ambitions and priorities:

- Council Ambitions – To prevent and/or detect crime or disorder, whilst respecting individuals rights under the European Convention on Human Rights (“**ECHR**”) and the Human Rights Act 1998 (“**HRA**”), and ensuring compliance with the Regulation of Investigatory Powers Act 2000 (“**RIPA**”).
- Community Objectives – None.
- Corporate Priorities – None.
- Other Considerations – None.

2. BACKGROUND

2.1 RIPA came into force on 25 September 2000; its aim is to strike a balance between protecting individuals' rights under Article 8 ECHR and the HRA and the need for investigatory powers to protect the interests of society as a whole. RIPA allows the Council to carry out directed surveillance and/or use covert human intelligence sources (“**CHIS**”) lawfully if it is authorised in accordance with the provisions of RIPA, it is necessary for the purpose of preventing or detecting crime or disorder, it is proportionate to the aims, which it seeks to achieve, and any authorisation receives judicial approval.

2.2 Until 1 September 2017 the Office of the Surveillance Commissioner (“**OSC**”) carried out routine inspections of all public bodies to ensure their compliance with the requirements of RIPA. On 1 September 2017, this passed to the Investigatory Powers Commissioner's Office.

2.3 Mrs Grainne Athorn (“**Inspector**”) carried out a paper exercise and concluded that a full inspection was not required. She did however make a number of comments and recommendations. A copy of the covering letter from Lord Justice Fulford dated 11 September 2017 and the Inspector's report setting out her findings and recommendations are enclosed at **Appendix 1** to this report (“**Inspection Report**”).

2.4 The Inspector made two recommendations in her report:

- The Requirement to complete a risk assessment prior to the authorisation and reauthorisation of a CHIS be added to the existing RIPA policy; and
- The corporate RIPA policy be further enhanced by the introduction of control measures to ensure that should it become necessary to utilise online covert identities/pseudonyms, these be centrally logged and a record made of what research activity is conducted, details of which should be reported to the relevant

2.6 In response to these recommendations the Council has amended its RIPA policy to incorporate all the recommended amendments set out in paragraph 13 of the Inspection Report. A copy of this is contained at **Appendix 2**.

3. RISK ASSESSMENT

3.1 The approval of this report may have the following implications:

- Resources – Resources have been expended in amending the policy and will be in providing RIPA training to the Chief Executive, and the Directors of the Council.
- Technical, Environmental and Legal – The Council will be better able to pursue legal action as necessary.
- Political – No implications identified.
- Reputation – The Council's response to the Inspection Report will demonstrate the Council's commitment to carrying out its responsibilities.

4. **RECOMMENDED THAT COMMITTEE**

4.1 Note the Inspector's recommendations.

4.2 Approve the amended policy with immediate effect.

MAIR HILL
SOLICITOR

MARSHAL SCOTT
CHIEF EXECUTIVE

SOLICITOR BACKGROUND PAPERS

Appendix 1 – Inspection Report

Appendix 2 – Amended Policy

For further information please ask for Mair Hill, on extension 3216.

IPCO

Investigatory Powers
Commissioner's Office

PO Box 29105, London

Chief Executive Mr Marshal Scott
Ribble Valley Borough Council
Council Offices
Church Walk
Clitheroe
Lancashire
BB7 2RA

11th September 2017

Dear Mr Scott

The inspection by Ms Gráinne Athorn was a marked success because of the cooperation she received on the part of all involved and the time taken to answer all the questions and matters that were raised. I am grateful to the Chief Executive, Mr Marshal Scott, and his team for their excellent approach. It is to be noted that no RIPA surveillance or CHIS activity has been requested since the last inspection in 2014; as a result the inspection was undertaken without a visit by Ms Athorn.

I extend my thanks for the assistance that was provided.

It is to be noted that the two recommendations made by HH David Hodson in 2014 have been implemented; these related to amendments to the corporate policy and training for the Chief Executive and the two relevant directors.

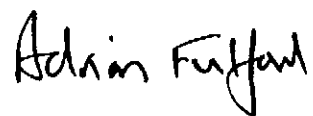
The overarching RIPA Policy merits praise, particularly as it is well written and organised, and contains all the relevant information. It is recommended that the Policy, in order to comply with the Covert Human Intelligence Source Code of Practice, should be amended to include the requirement that a risk assessment must be undertaken prior to authorisation/reauthorisation of a CHIS.

Furthermore, it is suggested that control measures are introduced to ensure that if covert identities or pseudonyms are used, they need to be centrally logged; further, a record needs to be made of the activity that is undertaken, and details should be reported to the relevant authorising officer.

I am pleased to note that the three designated authorising officers have completed their refresher training, and there is informal mentoring and an advisory service for RIPA-related matters.

Notwithstanding the few recommendations made in the inspection report, the authority is clearly taking its responsibilities seriously and I encourage this positive approach and the proper use of these powers.

Yours sincerely,

A handwritten signature in black ink that reads "Adrian Fulford". The signature is written in a cursive, slightly slanted style.

Lord Justice Fulford

OFFICIAL - SENSITIVE



OFFICE OF SURVEILLANCE COMMISSIONERS
INSPECTION REPORT

Ribble Valley Borough Council

14th August 2017

**Surveillance Inspector:
Mrs Grainne Athorn**

OFFICIAL - SENSITIVE

OFFICIAL- SENSITIVE

DISCLAIMER

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

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

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

The report is sent only to the recipient of the Chief Surveillance Commissioner's letter (normally the Chief Officer of the authority inspected). Copies of the report, or extracts of it, may be distributed at the recipient's discretion but the version received under the covering letter should remain intact as the master version.

The Office of Surveillance Commissioners is not a public body listed under the Freedom of Information Act 2000, however, requests for the disclosure of the report, or any part of it, or any distribution of the report beyond the recipients own authority is permissible at the discretion of the Chief Officer of the relevant public authority without the permission of the Chief Surveillance Commissioner. Any references to the report, or extracts from it, must be placed in the correct context.

OFFICIAL – SENSITIVE



OSC INSP/075

The Rt. Hon. Lord Judge
Chief Surveillance Commissioner
Office of Surveillance Commissioners
PO Box 29105
London SW1V 1ZU

14th August 2017

OSC INSPECTION – RIBBLE VALLEY BOROUGH COUNCIL

1 Date of Inspection

A desktop review of Ribble Valley Borough Council was undertaken on Monday 14th August 2017.

2 Inspector

Mrs Gráinne Athorn.

3 Introduction

3.1 Ribble Valley is a local government district with borough status in the county of Lancashire. Geographically it covers a large area including the Forest of Bowland to the north, Gisburn in the east and Longridge in the west. Clitheroe is the largest town in the area and is home to the Ribble Valley administration.

3.2 The current Chief Executive is Mr Marshal Scott who is supported by Directors of Community Services and Finance, both of whom are designated and trained Authorising Officers. The SRO is Mair Hill a solicitor by profession who has oversight of all RIPA related activity undertaken by the council.

3.3 The address for correspondence is Council Offices, Church Walk, Clitheroe, Lancashire, BB7 2RA.

4 Inspection Approach

4.1 The last inspection was undertaken during 2014 by HH David Hodson an Assistant Surveillance Commissioner. In the period since the last inspection no RIPA surveillance or CHIS activity has been requested or authorised. As a consequence this report has been prepared without visiting Ribble Valley Borough Council. To assess the ongoing compliance of the council, information provided by the SRO has been reviewed which included a RIPA Policy and draft amended RIPA Policy due for publication during September 2017.

OFFICIAL

- ii. In respect of CHIS, The Covert Human Intelligence Source Code of Practice states that a risk assessment must be prepared prior to the authorisation and deployment of a CHIS and be updated frequently throughout their activity, thus ensuring that their welfare and safety is protected. **It is therefore recommended that the requirement to complete a risk assessment prior to the authorisation and reauthorisation of a CHIS be added to the existing RIPA Policy.**

- 6.3 The RIPA policy has recently been redrafted to include a new section concerning the access of private information available on the internet and social media during investigations. The statements contained within the draft correspond with guidance offered by the Surveillance Commissioners and accurately warn of the privacy implications of repeatedly accessing such information. The document further references that there may be an intention to access such information or profiles using covert identities or pseudonyms.

- 6.4 Information provided by the SRO in the course of this Inspection indicates that control is exercised over the number of Council employees who are permitted to access social media in conjunction with their professional duties, and of the thirteen staff permitted; only two are fulfilling investigative roles. Both individuals have been provided with bespoke guidance by the SRO as per the advice contained within the revised policy.

- 6.5 Whether or not Ribble Valley chooses to sanction the use of covert online identities is a matter for its leaders, however it is important that if such activity is undertaken in conjunction with a Directed Surveillance Authorisation, it is done in a manner that is both controlled and effectively overseen by managers and the relevant Authorising Officer. As such **it is recommended that this guidance be further enhanced by the introduction of control measures to ensure that should it become necessary to utilise online covert identities/pseudonyms, these be centrally logged and a record made of what research activity is conducted, details of which should be reported to the relevant Authorising Officer during routine reviews or, where applicable, a cancellation.**

- 7 Training**

- 7.1 Since the last Inspection in 2014 all three designated Authorising Officers have completed refresher training and all are due to do so again this year. In addition to the delivery of formal training, the SRO provides a more informal mentoring and advisory service for staff members seeking to develop their knowledge of RIPA matters. To ensure a consistent level of knowledge between the AOs and SRO it is suggested that he be invited to join them during the next training event.

- 8. Reports to Members**

- 8.1 RIPA matters are the subject of oversight by Members of the Policy and Finance Committee. From September 2017 RIPA matters including usage figures will be provided on a six monthly rather than annual basis.

OFFICIAL

- 12.3 The amendments to the RIPA Policy suggested within this report relating to social media and the use of covert identities reflect a progression of operating practice that would bring Ribble Valley into line with other practitioners.
- 12.4 In respect of the required changes in relation to CHIS, amending the policy in the manner suggested will enable any officer applying for an authorisation for a CHIS (no matter how remote the possibility) to do so in such a way that is lawful and protects the source in question.
- 12.5 The planned refresher training for AOs will continue to ensure Ribble Valley's continued readiness to utilise its covert investigative powers should it become necessary to do so in the future, particularly if the decision is taken to utilise online information.
- 12.6 The absence of authorisation documentation generated since the last inspection means that it is not possible to comment upon the quality of authorisations, however should one be required there appears sufficient guidance available to enable it to be completed to a good standard.

13 Recommendations

- 13.1 The requirement to complete a risk assessment prior to the authorisation and reauthorisation of a CHIS be added to the existing RIPA Policy.
- 13.2 The corporate RIPA Policy be further enhanced by the introduction of control measures to ensure that should it become necessary to utilise online covert identities/pseudonyms, these be centrally logged and a record made of what research activity is conducted, details of which should be reported to the relevant Authorising Officer during routine reviews or, where applicable, a cancellation.

Gráinne Athorn
Surveillance Inspector

Corporate Policy in Respect of Regulation of Investigatory Powers Act 2000 (“RIPA”)



Ribble Valley
Borough Council

www.ribblevalley.gov.uk

NOVEMBER 2017

INDEX

Item	Description	Page
1.	Introduction	3
2.	Legislative Background	3-7
3.	Surveillance	7-9
4.	Covert Human Intelligence Sources	9-12
5.	Authorisation Process	12-19
6.	Authorising Officers	19-20
7.	Records and Central Register	20-21
8.	Complaints	22
9.	Appendices	
	• Appendix 1 - Code of Conduct on Directed Surveillance	22
	• Appendix 2 – Code of Conduct on Covert Human Intelligence Sources	22
	• Appendix 3 – Home Office Guidance to Local Authorities in England and Wales on the judicial approval process for RIPA and the crime threshold for directed surveillance	22

1. INTRODUCTION

- 1.1 This Corporate Policy is based upon the requirements of the Regulation of Investigatory Powers Act 2000 (“**RIPA**”), the Home Office’s Code of Practice for Covert Surveillance and property interference, and Covert Human Intelligence Sources (“**CHIS**”) (“**Codes**”), and the Home Office guidance for local authorities in England and Wales on the judicial approval process for RIPA and the crime threshold for directed surveillance (“**Guidance**”).
- 1.2 Ribble Valley Borough Council (the “**Council**”) has also taken into account and incorporated the guidance given by the Office of Surveillance Commissioners in its report dated 4 June 2008, 21 August 2011, and 10 August 2014 and is grateful to it for providing this.
- 1.3 On 18 November 2008 the Head of Legal and Democratic Services was authorised by the Council’s Policy and Finance Committee to carry out periodic reviews of this policy and to amend it to the extent necessary to keep it up to date and in line with the Home Office’s Codes of Practice. As recommended in the Codes an annual report will be taken to the Council’s Policy and Finance Committee, which will contain such detail to enable Committee to determine that the Council’s policy is fit for purpose. There will also be 6 monthly reports to Committee on the level of RIPA activity or inactivity.
- 1.4 Whilst this policy provides guidance it is not intended to be an authoritative source on the provisions of RIPA. All Officers must therefore make reference to RIPA itself and to the Codes, and the Guidance for an authoritative position.
- 1.5 Should any Officer be uncertain in respect of any aspect of RIPA, the authorising procedures set out in this policy, or at all, they should contact the legal department of the Council immediately.
- 1.6 The Council’s Solicitor is the RIPA Senior Responsible Officer.

2. LEGISLATIVE BACKGROUND

2.1 The Human Rights Act 1998 (the “**HRA**”) incorporated the European Convention on Human Rights (the “**ECHR**”) into domestic law.

2.2 Article 8 of the ECHR provides that:

“1. *Everyone has the right to respect for his private and family life, his home and his correspondence.*

2. *There shall be no interference by a public authority with the exercise of this right except such as is **in accordance with the law** and is **necessary** in a democratic society in the interests of national security, public safety or the economic well being of the country, for the prevention of disorder or crime, for the protection of health or morals or for the protections of the rights and freedoms of others.” [Emphasis added]*

2.3 There is therefore a qualified right for interference with individual’s rights under Article 8 if it is:

2.3.1 done in accordance with the law;

2.3.2 necessary; and/or

2.3.3 proportionate.

2.4 Any individual undertaking surveillance and/or using CHIS on behalf of the Council will therefore be breaching a person’s human rights unless that surveillance is authorised in accordance with the law, is necessary for one of the reasons set out above, and is proportionate.

2.5 This could have serious implications for the Council, not only in terms of its reputation, but could also potentially render any evidence gathered during the surveillance inadmissible in criminal proceedings, leave the Council open to civil proceedings for a breach of an individual’s human rights, and/or lead to a complaint being made to the Ombudsman. To avoid such a situation arising therefore, Officers must not carry out either Surveillance and/or CHIS unless the provisions of paragraph 2.3 are complied with.

In accordance with the law – RIPA

- 2.6 RIPA came into force on 25 September 2000, with the Codes subsequently coming into force pursuant to Section 71 of RIPA. The aim of RIPA was to strike a balance between protecting individuals' rights under Article 8 ECHR and the HRA and the need for investigatory powers to protect the interests of society as a whole. It therefore allows interference with individuals' rights in certain circumstances.

Necessity

- 2.7 It should be noted that pursuant to the Regulation of Investigatory Powers (Directed Surveillance and Covert Human Intelligence Sources) Statutory Instrument No. 2010/521 ("**RIPA Order 2010**") a local authority, (and hence the Council) can only rely on Section 28 (3) (b) of RIPA as a ground for its interference being necessary. Therefore, under RIPA any interference can **only** be necessary if it is "*for the purpose of preventing or detecting crime where the offence is punishable by a maximum term of at least six months imprisonment.*"
- 2.8 Regulation 7A of the 2010 RIPA Order (as amended by the 2012 RIPA Order SI 2012/1500) introduced this further limitation so that Authorising Officers may only authorise surveillance in respect of a criminal offence which is punishable by a maximum term of at least 6 months imprisonment or which constitutes an offence under section 146, 147 or 147A of the Licensing Act 2003 (sale of alcohol to children) or section 7 of the Children and Young Persons Act 1933 (sale of tobacco to children under 18 years old).
- 2.9 However, not all applications for the purpose set out above will be necessary. The Authorising Officer **must** be satisfied that it is necessary in all the circumstances. A judgment will have to be made on a case-by-case basis. Generally any such interference will not be necessary if there is an alternative **overt** method which could be used to obtain the information. Authorising Officers should therefore satisfy themselves that all other methods have either been exhausted or are not practicable. Authorising Officers should also take care to record in the authorisation their reasoning as to why the action is necessary.

Proportionate

- 2.10 Once it has been established that such interference is necessary it must then be considered whether it is **proportionate** to what is to be achieved. The Authorising Officer should consider the following elements of proportionality (as set out in paragraph 3.6 of the Code):
- 2.10.1 Balancing the size and scope of the proposed activity against the gravity and extent of the perceived crime or offence;
 - 2.10.2 Explaining how and why the methods to be adopted will cause the least possible intrusion on the subject and others;
 - 2.10.3 Considering whether the activity is an appropriate use of the legislation and a reasonable way, having considered all reasonable alternatives, of obtaining the necessary result; and
 - 2.10.4 Evidencing as far as reasonably practicable what other methods had been considered and why they were not implemented.
- 2.11 Authorising Officers should also take care to record within the authorisation form the reasons why they consider that the action is proportionate.

Judicial Approval

- 2.12 Following authorisation by an Authorising Officer judicial approval must be obtained prior to any surveillance being undertaken. Section 32A(2) of RIPA states that “*The authorisation is not to take effect until such time (if any) as the relevant judicial authority has made an order approving the grant of the authorisation.*”
- 2.13 Section 32A(3) of RIPA further provides that:
- “(3) The relevant judicial authority may give approval under this section to the granting of an authorisation under section 28 if, and only if, the relevant judicial authority is satisfied that-*
- at the time of the grant-*
- there were reasonable grounds for believing that the requirements of section 28(2) were satisfied in relation to the authorisation, and*
- the relevant conditions were satisfied in relation to the authorisation, and*

at the time when the relevant judicial authority is considering the matter, there remain reasonable grounds for believing that the requirements of section 28(2) are satisfied in relation to the authorisation.

(4) For the purposes of subsection (3) the relevant conditions are –

(a) in relation to a grant by an individual holding an office, rank or position in a local authority in England or Wales, that-

the individual was a designated person for the purposes of section 28,

the grant of the authorisation was not in breach of any restrictions imposed by virtue of section 30(3), and

any other conditions that may be provided for by an order made by the Secretary of State were satisfied,.....”.

- 2.14 The procedure for making an application for judicial approval is contained in *The Magistrates’ Court (Regulation of Investigatory Powers) Rules 2012 (SI 2012/2563*, and is explained further in the Guidance.

3. SURVEILLANCE

What is surveillance?

- 3.1 Surveillance includes:

3.1.1 Monitoring, observing, listening to persons, watching or following their movements, listening to their conversations and other such activities or communications;

3.1.2 Recording anything mentioned above in the course of authorised surveillance; and/or

3.1.3 Surveillance, by or with, the assistance of appropriate surveillance device(s).

- 3.2 Surveillance can be either overt or covert.

Overt Surveillance

- 3.3 The vast majority of surveillance, which the Council carries out, will be overt and will involve Officers and employees noting events in the course of their normal daily duties. This will not fall within the scope of RIPA and will not require an authorisation. For example, a dog warden who notes an offence being committed as he/she carries out their daily routine will not require RIPA authorisation.

Covert Surveillance

- 3.4 Covert surveillance is defined in section 26(9)(a) of RIPA. It provides that *“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”*.

Covert Surveillance of Social Networking Sites (SNS)

- 3.5 Occasionally officers may be alerted to information on social media which may be pertinent to an investigation. When using social media sites for gathering evidence to assist in enforcement activities, officers should note that the fact that digital investigation is routine or easy to conduct does not reduce the need for authorisation. Care must be taken to understand how the specific SNS being used works particularly in relation to privacy settings.

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 authority, it is unwise to routinely regard it as ‘open source’ or publicly available. The author has a reasonable expectation of privacy if access controls are applied. Where privacy settings are available but not applied the data may be considered open source and an authorisation is not usually required. Repeat viewing of ‘open source’ sites may constitute directed surveillance and this should be borne in mind. To ensure compliance with regulations:

- Officers must **not** create a false identity in order to ‘befriend’ individuals on social media networks without authorisation under RIPA. If it is necessary and proportionate for the Council to covertly breach access controls, an authorisation for Directed Surveillance will be required. An authorisation for the use and

conduct of a CHIS is necessary if a relationship is established or maintained by the officer.

- Officers viewing an individual's public profile on a social network should do so only to the minimum degree necessary and proportionate.
- Legal advice should be taken in advance as to whether repeated viewing of open profiles on social networks to gather evidence or to monitor an 'individual's' status for a specific investigation will require RIPA authorisation.
- Officers should also be aware that it is not possible to verify the accuracy of information on social networking sites, and if such information is to be used as evidence, take reasonable steps to ensure its validity.

In the event that it is necessary to utilise online covert identities/pseudonyms, pursuant to a RIPA authorisation, these must be centrally logged by the Senior Responsible Officer and a record made of what research activity is conducted, details of which should be reported to the relevant Authorising Officer during routine reviews or, where applicable, a cancellation.

RIPA Part II

3.5 RIPA Part II applies to the following conduct:

- 3.5.1 Directed Surveillance
- 3.5.2 Intrusive surveillance
- 3.5.3 Covert Human Intelligence Sources

Directed Surveillance (Section 26(2) RIPA)

3.6 **Section 26(2)** defines directed surveillance as surveillance, which is:

- 3.4.1 Covert but not intrusive;
- 3.4.2 Undertaken for the purpose of a specific operation;

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

3.4.5 Otherwise than by way of an immediate response to events or circumstances the nature of which is such that it would not be reasonably practicable for an authorisation under this Part to be sought for the carrying out of surveillance.

3.7 **Section 26(10)** defines “private information” in relation to a person as *“including any information relating to his private or family life”*.

Private information should be taken generally to include any aspect of a person’s private or personal relationship with others, including family and professional or business relationships. Family should be treated as extending beyond the formal relationships created by marriage or civil partnerships.

Intrusive Surveillance (Section 26(3)-(6))

3.8 **Section 26(3)** defines surveillance as intrusive if and only if it is covert surveillance that:

3.8.1 Is carried out in relation to anything taking place on any residential premises or in any private vehicle; and

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

3.9 Pursuant to **Section 26 (5)** surveillance which:

39.1 Is carried out by means of a surveillance device in relation to anything taking place on a residential premises or in any private vehicle, but

3.9.2 Is carried out without that device being present on the premises or in the vehicle.

is not intrusive **unless** the device is such that it consistently provides information of the same quality and detail as might be expected to be obtained from a device actually present on the premises or in the vehicle.

3.10 Please note that there is **NO** provision for a local authority to authorise intrusive surveillance.

4. COVERT INTELLIGENCE SOURCES (“CHIS”)

Who is a CHIS?

4.1 **Section 26(8)** of RIPA defines a CHIS as a person 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 (b) & (c) below;
- (b) covertly uses such a relationship to obtain information or to 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.

4.2 This is defined further within **Section 26(9)(b)&(c)** so that:

4.2.1 A **purpose** will only be covert if, and only if, it is carried out in a manner that is calculated to ensure that one of the parties to the relationship is unaware of the purpose.

4.2.2 A **relationship** is used **covertly**, and information obtained 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.

- 4.3 Hence, there is no use of CHIS if a member of the public offers information to the Council that may be material to an investigation of an offence, but there would be if the Council then asked that person to obtain further information.

Authorising a CHIS

- 4.4 An authorisation **must** be obtained for CHIS in the same way as for directed surveillance. A detailed explanation of the authorisation process is contained in **Section 5** below. However, in addition, to the process for considering whether an authorisation is justified, a CHIS should not be authorised if it does not comply with the requirements of **Section 29(5)** of RIPA.

- 4.5 **Section 29(5)** requires that:

4.5.1 There will at all times be a person holding an office, rank, or position with the relevant investigating authority who will have **day to day responsibility for dealing with the source** on behalf of that authority, and **for the source's security and welfare ("Handler")**;

4.5.2 There will at all times be another person holding an office, rank or position with the relevant investigating authority who will have **general oversight** of the use made of the source ("**Controller**");

4.5.3 There will at all times be another person holding an office, rank or position with the relevant investigating authority who will have responsibility for **maintaining a record** of the use made of the source;

4.5.4 The records relating to the source that are maintained by the relevant investigating authority will always contain particulars of all such matters (if any) as may be specified for the purposes of this paragraph in regulations made by the Secretary of State (**see below**); and

4.5.5 The records maintained by the relevant investigating authority that disclose the identity of the source will not be available to persons except to the extent that there is a need for access to them to be made available to those persons.

- 4.6 With regard to paragraph 4.5.4 above the regulations are set out in the Regulation of Investigatory Powers (Source Records) Regulations 2000. These regulations can be found at www.security.homeoffice.gov.uk/ripa/legislation/ripa-statutory-instruments, and **must** be referred to by Officers.

Security and Welfare

Before authorising the use of conduct of a CHIS the authorising officer should ensure that a risk assessment is carried out to determine the risk to the CHIS of any tasking and the likely consequences should the role of CHIS become known.

The ongoing security and welfare of the CHIS, after cancellation of the authorisation should also be considered at the outset. Also consideration should be given to the management of any requirement to disclose information tending to reveal the existence or identity of a CHIS to, or at court.

The Handler will be responsible for bringing to the attention of the Controller any concerns about the personal circumstances of the CHIS in so far as they might affect:

- The validity of the risk assessment;
- The conduct of the CHIS; and
- The safety and welfare of the CHIS.

Where appropriate concerns about such matters must be considered by the authorising officer, and a decision taken on whether or not to allow the authorisation to continue.

Vulnerable Individuals

- 4.7 A vulnerable individual is a person who is or may be in need of community care services by reason of mental or other disability, age, illness and who is or may be unable to take care of himself, or unable to protect himself against significant harm or exploitation.

Vulnerable individuals should only be authorised to act as a source in the most exceptional circumstances, and the Chief Executive may only give such an authorisation.

Juvenile sources

- 4.8 There are also special safeguards with regard to the use or conduct of juvenile sources (under 18 years).
- 4.9 A source under 16 years of age **must not** be authorised to give information against his parents or any person who has parental responsibility for him.
- 4.10 There are also further requirements within the Regulation of Investigatory Powers (Juveniles) Order 2000 (SI No. 2793), and in other cases authorisations should not be granted unless these provisions are complied with. A copy of this can be also be found at www.security.homeoffice.gov.uk/ripa/legislation/ripa-statutory-instruments, and must be referred to by all Officers
- 4.11 The duration of such an authorisation is **one month** instead of 12 months.
- 4.12 Notwithstanding the above, the Council has not to date utilised these powers and considers that it is rare that they would be used in the future. As such **only** the **Chief Executive** may authorise any application for the use of CHIS and Officers should contact the legal department before making any application.

5. AUTHORISATION PROCESS

- 5.1 Directed surveillance and/or the use of CHIS shall be lawful for all purposes, if the conduct is properly and legitimately authorised and an Officer's conduct is in accordance with the authorisation.
- 5.2 Therefore all officers must obtain an authorisation from an Authorising Officer and Judicial approval before undertaking either directed surveillance and/or the use of CHIS, to ensure that it is lawful. A flowchart setting out the steps to be taken is contained at page 17 of the Guidance which can be found at **Appendix 3**.
- 5.3 Authorisations will only be given where:

- 5.3.1 The directed surveillance and/or the use of CHIS is necessary in the interests of preventing or detecting crime or disorder where the offence is punishable by a maximum term of at least six months imprisonment; and
- 5.3.2 It is proportionate to the objective which it is intended to achieve.
- 5.4 The Authorising Officer **must** satisfy himself of this before granting the authorisation.
- 5.5 In particular the Authorising Officer must consider whether the activity could be carried out in an overt or less intrusive manner. If it could then this should be the preferred method.

Collateral Intrusion

- 5.6 Before granting an authorisation an Authorising Officer **must** take into account the risk of intrusion into the privacy of persons other than those who are directly the subjects of the investigation or operation.
- 5.7 Wherever practicable measures should also be taken, to avoid or minimise unnecessary intrusion into the lives of those people.
- 5.8 The applicant should also have included an assessment of the risk of collateral intrusion in the application form and the Authorising Officer should consider this in making their decision.

Confidential Information

- 5.9 RIPA does not provide any special protection for “confidential information”.
- 5.10 Notwithstanding this, special care should be taken where the subject of the investigation or operation might reasonably expect a high degree of privacy or where confidential information may be involved.
- 5.11 Confidential information includes, matters subject to legal privilege, confidential personal information or confidential journalistic material.

- 5.12 For example special care should be taken with **surveillance** where it would be possible to acquire knowledge of discussions between a minister of religion and an individual relating to the latter's spiritual welfare, or where matters of medical or journalistic confidentiality or legal privilege may be involved.
- 5.13 In cases where through the use of surveillance and/or CHIS, confidential information may be obtained, **only** the Chief Executive, or in his absence, a Director, may give authorisation.

Application Forms

- 5.14 All applications and authorisations **must** be made/granted on the relevant Home Office forms. Electronic copies of these forms are available on the Home Office website at **www.security.homeoffice.gov.uk/ripa/publication-search/ripa-forms** If an officer has difficulty obtaining the correct form they should contact the Legal Department.

Content of Application

- 5.15 The applicant must ensure that each application contains a **unique reference number** ("URN"). This must be inserted into the box at the top right hand corner of the relevant form. This should include a reference to their department, the year, and the number of the application during that year. Authorising Officers should not authorise any application, which does not contain this.
- 5.16 Applicants must also ensure that they complete all boxes within the forms. If done properly this will ensure compliance with RIPA's requirements. However, to ensure that there is full compliance the details of RIPA's requirements are set out below.

Application for Directed Surveillance

- 5.17 A written application for directed surveillance should include:
- 5.17.1 the reason(s) why the authorisation is necessary in the particular case and the ground(s) on which it is considered necessary pursuant to Section 28(3)

of the Act. As set above the only ground on which the Council can now rely is “*for the purpose of preventing or detecting crime or disorder*”.

- 5.17.2 the reasons why the surveillance is considered proportionate to what it seeks to achieve;
- 5.17.3 the nature of the surveillance;
- 5.17.4 the identities, where known of those to be the subject of the surveillance;
- 5.17.5 an explanation of the information, which it is desired to obtain as a result of the surveillance;
- 5.17.6 the details of any collateral intrusion and why the intrusion is justified;
- 5.17.7 the details of any confidential information that is likely to be obtained as a consequence of the surveillance;
- 5.17.8 the level of authority required (or recommended where that is different) for the surveillance; and
- 5.17.9 a subsequent record of whether authorisation was given or refused, by whom, and the date and time.

Application for the use of CHIS

- 5.18 An application for the use or conduct of a source should include:
 - 5.18.1 the reasons why the authorisation is necessary, and the grounds listed in section 29(3). Again, the only ground upon which the Council can rely is “*for the purpose of preventing or detecting crime where the offence is punishable by a maximum term of at least six months imprisonment*”;
 - 5.18.2 the reasons why the authorisation is considered proportionate to what it seeks to achieve;

- 5.18.3 the purpose for which the source will be tasked or deployed;
- 5.18.4 where a specific investigation or operation is involved, the nature of that investigation or operation;
- 5.18.5 the nature of what the source will be tasked to do;
- 5.18.6 the level of authority required (or recommended where different);
- 5.18.7 the details of any potential collateral intrusion and why the intrusion is justified;
- 5.18.8 the details of any confidential information that is likely to be obtained as a consequence of the authorisation; and
- 5.18.9 a subsequent record of whether authority was given or refused, by whom and the time and date.

Duration Of Authorisations

Directed Surveillance

- 5.19 A written authorisation granted by an Authorising Officer will cease to have effect (unless renewed) at the end of a period of **three months** beginning with the day on which it took effect.

CHIS

- 5.20 A written authorisation will unless renewed cease to have effect at the end of a period of **twelve months** beginning with the day on which it took effect.

Reviews

- 5.21 Regular reviews should be carried out to assess the need for the authorisation to continue. Reviews should take place frequently if the source of surveillance provides confidential information or involves collateral intrusion.
- 5.22 The Authorising Officer must decide how frequently and when the reviews should take place. This should be as frequently as is considered necessary and practicable.
- 5.23 The Authorising Officer must use the appropriate form to complete the review, and the results of the review should be recorded in the central record of authorisations.

Renewals

- 5.24 If at any time before an authorisation ceases to have effect an Authorising Officer considers it necessary for the authorisation to continue for the purpose for which it was given he may renew it for:
 - 5.28.1 3 months (Directed Surveillance)
 - 5.28.2 12 months CHIS
- 5.25 The renewal will take effect at the time at which, or the day on which the authorisation would have ceased to have effect but for the renewal.
- 5.26 An application for renewal of an authorisation should not be made until shortly before the authorisation is due to cease to have effect.
- 5.27 Any person who would be entitled to grant a new authorisation is able to renew an authorisation.
- 5.28 An authorisation can be renewed more than once as long as it continues to meet the criteria for authorisation.
- 5.29 The application for renewal must include:
Directed Surveillance

- Whether this is the first renewal of an authorisation on which the authorisation has been renewed previously;
- Any significant changes to the information included in the initial application;
- The reasons why the authorisation for directed surveillance should continue;
- The content and value to the investigation or operation of the information so far obtained by the surveillance; and
- The results of regular reviews of the investigation or operation.

CHIS

- Whether this is the first renewal or every occasion on which the authorisation has been renewed previously;
- Any significant changes to the information in the original application;
- The reasons why it is necessary to continue to use the source;
- The use made of the source in the period since the grant or, as the case may be, latest renewal of the authorisation;
- The tasks given to the source during that period and the information obtained from the conduct or use of the source; and
- The results of regular reviews of the use of the source.

5.30 **As with new applications judicial approval must also be sought after the Authorising Officer gives authorisation.**

Cancellations

- 5.31 The Authorising Officer who granted or last renewed the authorisation **must** cancel it if he is satisfied that it no longer meets the criteria under which it was first granted.
- 5.32 The Authorising Officer must complete the relevant form to do so and pass the information to the legal department to be included on the central register.
- 5.33 In addition, when the decision is taken to stop surveillance, an immediate instruction must be given to those involved to stop all surveillance of the subject(s). The date and time when such an instruction was given should be recorded in the central register and on the cancellation form.
- 5.34 There is no requirement for any further details to be recorded when cancelling a directed surveillance authorisation but effective practice suggests that a record should be retained detailing the product obtained from the surveillance and whether or not objectives were achieved.

6. AUTHORISING OFFICERS

- 6.1 The Regulation of Investigatory Powers (Directed Surveillance and Covert Human Intelligence Sources) Order 2010 SI 2010 No. 521 provides that the Director, Head of Service, Service Managers, or equivalent officer may give authorisations for directed surveillance and CHIS under RIPA.
- 6.2 In light of the infrequent use made of RIPA and CHIS and based on advice given by the OSC, Ribble Valley Borough Council has resolved that it will only have three Authorising Officers who will be the Chief Executive, the Director of Community Services, and the Director of Resources. These Officers will receive regular training to enable them to deal properly with all authorisations.
- 6.3 Moreover, applicants must submit their application to an Authorising Officer, from outside of their department.

7. RECORDS AND CENTRAL REGISTER

- 7.1 The Council's Legal Department will maintain a central record of all authorisations. This will be updated whenever an authorisation is granted, renewed, or cancelled.
- 7.2 The record will be retained for a period of at least **three years** from the end of the authorisation and will contain the following information:
- 7.2.1 the type of authorisation;
 - 7.2.2 the date the authorisation was given;
 - 7.2.3 Name and rank/grade of the authorising officer,
 - 7.2.4 the unique reference number (URN) of the investigation or operation;
 - 7.2.5 the title of the investigation or operation, including a brief description and names of subjects, if known;
 - 7.2.6 details of attendances at the magistrates' court to include the date of attendances at court, the determining magistrate, the decision of the court and the time and date of that decision;
 - 7.2.7 the dates of any reviews;
 - 7.2.8 if the authorisation is renewed, when it was renewed and who authorised the renewal, including the name and rank/grade of the Authorising Officer;
 - 7.2.9 whether the investigation or operation is likely to result in obtaining confidential information as defined in this code of practice;
 - 7.2.10 whether the authorisation was granted by an individual directly involved in the investigation; and
 - 7.2.11 the date the authorisation was cancelled.

- 7.3 In respect of each step in the procedure Authorising Officers **must** retain all original documentation **and must** give to the legal department a copy of the following information:
- 7.3.1 the application, and authorisation together with any supplementary documentation and notification of the approval given by the authorising officer;
 - 7.3.2 a record of the period over which the surveillance has taken place;
 - 7.3.3 the frequency of reviews prescribed by the authorising officer;
 - 7.3.4 a record of the result of each review of the authorisation;
 - 7.3.5 the renewal of an authorisation, given together with the supporting documentation submitted when the renewal was requested;
 - 7.3.6 the date and time when any instruction to cease surveillance was given; and
 - 7.3.7 the date and time when any other instruction was given by the authorising officer.
 - 7.3.8 A copy of the order approving or otherwise the grant or renewal of an authorisation from a Justice of the Peace (JP).
- 7.4 For the avoidance of doubt the information set out above must be passed to the legal department contemporaneously to ensure that the Council's central record can be maintained and that the Council can therefore ensure that all authorisations are reviewed and cancelled in accordance with RIPA.

8. **COMPLAINTS**

- 8.1 Any person who reasonably believes that they have been adversely affected by surveillance activity and/or the use of a CHIS, by or on behalf of the Council may

complain to the Head of Legal and Democratic Services (as Monitoring Officer) who will investigate the complaint.

8.2 They may also complain to:

The Investigatory Powers Tribunal
PO Box 33220
London SW1H 9ZQ

020 7035 3711

9. APPENDICES

1.	Code of Practice on Covert Surveillance - *www.security.homeoffice.gov.uk/ripa/publication-search/ripa-cop/
2.	Code of Practice on Covert Human Intelligence Sources - *www.security.homeoffice.gov.uk/ripa/publication-search/ripa-cop/
3.	Home Office Guidance to local authorities in England and Wales on the judicial approval process for RIPA and the crime threshold for directed surveillance – *www.gov.uk/government/uploads/system/uploads/attachment_data/file/118173/local-authority-england-wales.pdf