

Subject:	Updated RIPA Policy		Status:	For Publication	
Report to:	Cabinet		Date:	13 th October 2021	
Report of:	Head of Legal (Monitoring Officer)		Portfolio Holder:	Corporate Services	
Key Decision:	<input type="checkbox"/>	Forward Plan	<input checked="" type="checkbox"/>	General Exception	<input type="checkbox"/> Special Urgency
Equality Impact Assessment:		Required:	No	Attached:	No
Biodiversity Impact Assessment		Required:	No	Attached:	No
Contact Officer:	Clare Birtwistle		Telephone:	01706 252527	
Email:	clarebirtwistle@rossendalebc.gov.uk				

1.	RECOMMENDATION
1.1	To consider the recommendations of Overview and Scrutiny Committee and approve the updated RIPA policy 2021
1.2	Any future minor amends to the policy to be delegated to the Monitoring Officer in consultation with the Portfolio Holder.

2. PURPOSE OF REPORT

- 2.1 To note the recommendations of Overview and Scrutiny Committee and approve the updated RIPA policy.
- 2.2 To note the findings of the IPCO Inspection.

3. BACKGROUND

- 3.1 The Regulation of Investigatory Powers Act 2000 (“RIPA”) enables local authorities to carry out certain types of surveillance activity, as long as certain procedures are followed, which can be relied upon in court proceedings. In order to ensure that the procedures are followed, it is important to have an up to date policy which is understood by authorising officers and investigating officers. Members are required to regularly review the use of RIPA to ensure that the policy remains fit for purpose and all authorisations granted under the terms of it are in compliance to avoid challenge. The Council’s use of RIPA is reported to Overview and Scrutiny as part of the performance monitoring framework.
- 3.2 **Proposed Amends**
The RIPA Policy at Appendix 1 has been amended to take account of revised Home Office Codes of Practice, legislative changes affecting authorisations for juveniles used as Covert Human Intelligence Sources (CHIS) and to reflect changes to certain designations and regulators under the policy. Minor amends have previously been delegated to officers in consultation with the Portfolio Holder but this current refresh goes beyond that which is considered minor.
- 3.3 As a result of the Regulation of Investigatory Powers (Juveniles) (Amendment) Order 2018 coming into force on 20 July 2018, the authorisation period for juveniles used as CHIS has been increased from one month to four months subject to at least monthly reviews. A CHIS is someone employed to establish a relationship with another person for the purpose of covertly gathering evidence. The Police act as the lead authority in this type of work and the Council does not currently make use of CHIS, but it remains important that our policy reflects the changes that apply to the use of juvenile CHIS.

- 3.4 References in the policy about the Office of Surveillance Commissioners have also been changed to the Investigatory Powers Commissioner's Office (IPCO) which now has strategic oversight of the use of RIPA by local authorities.
- 3.5 Additional guidance has been inserted into the policy in relation to online covert activity eg the use of social media as a means to collecting information. This is a useful tool and reminds officers that an authorisation for directed surveillance need only be sought where they are 'systematically collecting and recording information about a particular person or group'
- 3.6 Following on from previous inspections the policy has also been amended in terms of the Authorising Officers to bring up to date the present titles and to demonstrate that the Senior Responsible Officer is now sufficiently independent from the appointed Authorising Officers.
- 3.7 Following comments at Overview and Scrutiny gender specific references have also been amended to be gender neutral.

3.8 **Inspection**

Given the drop in RIPA authorisations by local authorities generally since 2012, following the introduction of the serious crime threshold and requirement to seek approval from the Magistrates' Court, the inspection regime now adopted by IPCO is more of a desk top exercise, with on-site inspections only taking place where concerns about compliance with RIPA are found.

- 3.9 The Council was subject to a remote inspection by IPCO during February 2021. The results of the inspection can be found at Appendix 2. No formal recommendations were made as a result of that inspection and the Inspector was satisfied that all recommendations from the previous inspection had been discharged. The Inspector acknowledged that there had been no recent use of RIPA powers by the Council, the last being in October 2012, but they were reassured that the Council was still taking its responsibilities under RIPA seriously and together with the information that had been provided were satisfied that the Council had demonstrated a level of compliance that removed the requirement for a physical inspection.
- 3.10 During the inspection, the Inspector was asked to make comment on the draft policy and their comments have been taken on board.

4. **RISK**

- 4.1 Failure to have an up to date policy together with well-trained authorising and investigating officers could lead to legal challenge and the failure of legal proceedings taken against perpetrators.

Failure to maintain robust governance under the RIPA regime could also see the Council falling foul of the requirements of the IPCO and subject to a physical inspection.

5. **FINANCE**

- 5.1 There are no financial implications arising from the body of this report.

6. **LEGAL**

- 6.1 Where the Council wishes to carry out covert surveillance in relation to an investigation, compliance with RIPA ensures that any such surveillance is properly authorised and full consideration is given to its necessity and proportionality. Compliance with RIPA provides a

potential defence to any claim that the surveillance amounted to a breach of the individual's right to privacy under the Human Rights Act 1998. Whilst RIPA authorisations are limited to specific circumstances for local authorities, local authorities must still maintain appropriate processes and procedures to demonstrate compliance with RIPA, this includes ensuring that an appropriate policy document is maintained.

7. POLICY AND EQUALITIES IMPLICATIONS

7.1 No policy or equalities implications.

8. CONCLUSION

8.1 As set out in the body of the report it is necessary for the Council to review and refresh policies to avoid legal challenge and ensure practice and procedures are in line with legislation, codes of practice and good practice.

ROSSENDALE BOROUGH COUNCIL

REGULATION OF INVESTIGATORY
POWERS ACT 2000 (RIPA)

POLICY

Amended and approved by Council on 23rd March 2011
Amended by Director of Business in consultation with Councillor Robert Wilkinson, Portfolio Holder on 20th July 2011.
Amended by Director of Business in consultation with Councillor Sean Serridge, Portfolio Holder on 29th July 2014
Amended by Director of Business in consultation with Councillor Sean Serridge, Portfolio Holder on 29th October 2014

Other formats are available.
Please call 01706 217777 or
visit our One Stop Shop at
Futures Park, Bacup.

اردو বাংলা



	Legal	Version/Status	V1
responsible Author	Head of Legal (Monitoring Office) Legal Services Manager	Date Agreed / Agreed At	
Date last Amended	6th November 2018	Due for Review	

CONTENTS

1.	INTRODUCTION	3
2.	GUIDANCE – Part I – Direct Surveillance and CHIS.....	4
	(a) Scrutiny and Tribunal	4
	(b) Benefits of RIPA Authorisations	6
	(c) Definitions	6
	(d) When does RIPA apply	7
	(e) Covert Human Intelligence Source	8
	(f) Authorisations	9
	(g) Duration and Cancellation.....	15
	(h) Reviews	15
	(i) Renewals	16
	(j) Central Register of Authorisations	16
	(k) Retention of Records	17
	(l) Complaints Procedure	17
3.	GUIDANCE – Part II – Acquisition and Disclosure of Communications Data	17
	Introduction	17
	What is Communication Data	18
	Application Forms.....	18
	Authorisations	18
	Oral authority	19
	Duration	19
	Renewal and Cancellation	20
	Retention of Records	20
	Oversight and Complaints	20

APPENDICES

Appendix A	Directed Surveillance and CHIS Forms
Appendix B	Home Office Guidance to Local Authorities in England and Wales on the judicial approval process for RIPA and the crime threshold for directed surveillance
Appendix C	Home Office guidance for Magistrates' Courts in England and Wales for a local authority application seeking an order approving the grant or renewal of a RIPA authorisation or notice
Appendix D	HO - Codes of Practice – Covert Surveillance and Property Interference and Covert Human Intelligence Sources
Appendix E	Rosendale Borough Council's Authorising Officers
Appendix F	HO – Forms - Communications Data
Appendix G	HO - Codes of Practice - Acquisition and Disclosure of Communications Data

ROSSENDALE BOROUGH COUNCIL POLICY ON REGULATION OF INVESTIGATORY POWERS ACT 2000 (RIPA)

Introduction

Rossendale Borough Council (the Council) only carries out covert surveillance where such action is justified and endeavours to keep such surveillance to a minimum. It recognises the importance of complying with RIPA when such an investigation is for the purpose of preventing or detecting crime or preventing disorder and has produced this guidance document to assist officers.

Applications for Authority

All requests for authorisation of directed surveillance or a CHIS under RIPA must be approved in advance by an Authorising Officer. An Authorising Officer is a person who has been delegated power to act in that capacity. A list of officers who have, to date, been authorised, is annexed to this policy at Appendix E and is subject to regular review and updating by the Monitoring Officer in consultation with the Chief Executive and Directors/Director of Business. 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, and the serious crime threshold is met (see 6.2)
- the covert nature of the investigation is necessary
- proper consideration has been given to collateral intrusion
- the proposed length and extent of the surveillance is proportionate to the information being sought
- the authorisations are reviewed and cancelled
- the authorisations are sent to Legal Services for entry onto the Central Register.

Once authorisation has been obtained from the Authorising Officer, the Investigating Officer shall liaise with the Magistrates' Court to give prior notice of the need for a Judicial Approval and will then attend at Court, accompanied by a member of the Legal Services team, will attend the Magistrates' Court in order to obtain Judicial Approval for the authorisation.

Training

All officers with an enforcement or investigatory function should receive training on the provisions of RIPA to ensure awareness of the legislative framework and Council pPolicies and pPProcedures.

Central Register and Records

Legal Services shall facilitate and retain the Central Register of all authorisations issued by the Council. The Monitoring Officer~~Director of Business~~ will monitor the content of the application forms and authorisations to ensure conformity and compliance with RIPA.

RIPA GUIDANCE – PART I

DIRECTED SURVEILLANCE AND COVERT HUMAN INTELLIGENCE SOURCE

1. Purpose

The purpose of this guidance is to explain:

- the scope of RIPA – Chapter 1 of Part II
- the circumstances where it applies, and
- the authorisation procedures to be followed

2. Introduction

- 2.1 This Act which came into force in 2000 is intended to regulate the use of investigatory powers exercised by various bodies including local authorities, and ensure that they are used in accordance with human rights legislation. This is achieved by the requirement for certain investigations to be authorised by an appropriate officer together with judicial approval. From 1 November 2012 local authority authorisations and notices under RIPA will only be given effect once an order has been granted by a Justice of the Peace. See **Appendices C and D** for Home Office Guidance.
- 2.2 The investigatory powers which are relevant to a local authority are directed covert surveillance and covert human intelligence sources in respect of specific operations involving criminal offences that are either punishable, whether on summary conviction or indictment by a term of imprisonment of at least six months, or are related to the underage sale of alcohol and tobacco. The Act makes it clear for which purposes they may be used, to what extent, and who may authorise their use. There are Codes of Practice relevant to the use of these powers, the links to which are attached as **Appendix D**.
- 2.3 Consideration must be given, prior to authorisation as to whether or not the surveillance and associated collateral intrusion is **necessary** and **proportionate** i.e. whether a potential breach of human rights legislation is justified in the interests of the community as a whole, or whether the information could be gleaned in other ways.
- 2.4 The ~~Investigatory Powers Commissioners Office~~ ~~Office of Surveillance Commissioners~~ ~~has produced~~ publishes a restricted Procedures and Guidance Document to be used by local authorities <https://www.ipco.org.uk/docs/OSC%20PROCEDURES%20AND%20GUIDANCE.pdf>.
- 2.5 A public authority may only engage the 2000 Act when in performance of its **core functions**, that is the specific public functions undertaken by the authority in contrast to the ordinary functions that are undertaken by every authority for example employment issues, contractual arrangements etc.

3. Scrutiny and Tribunal

3.1 External

3.1.1 From 1 November 2012 the Council must obtain an Order from a Justice of the Peace approving the Grant or Renewal of any authorisation for the use of directed surveillance or CHIS before the authorisation can take effect and the activity carried out. The Council can only appeal a decision of a Justice of the Peace on a point of law by the Judicial Review process.

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

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

The Tribunal can order:

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

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

- granted any authorisation under RIPA
- engaged in any conduct as a result of such authorisation

3.2 Internal Scrutiny

3.2.1 The Council will ensure that a senior officer is responsible for:

- the integrity of the process in place within the Council to authorise directed surveillance and CHIS **Appendix E**
- compliance with Part II of the 2000 Act and with the accompanying Codes of Practice

- engagement with the Commissioners and Inspectors when they conduct their inspections and
- where necessary oversee the implementation of any post-inspection action plans recommended or approved by a Commissioner

3.2.2 The elected members of the Council will review the authority's use of the 2000 Act quarterly via the Corporate Overview and Scrutiny Committee. They will ensure that it is being used consistently with the Council's policy and that that policy is fit for purpose. The members will not however be involved in making decisions on specific authorisations.

Formatted: Indent: Left: 0.63 cm, No bullets or numbering

4. Benefits of RIPA authorisations

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

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

Section 78 Police and Criminal Evidence Act 1984 allows for the exclusion of evidence if it appears to the Court that, having regard to all the circumstances in which the evidence was obtained, the admission of the evidence would have such an adverse affect on the fairness of the proceedings that the Court ought not to admit it. Evidence obtained through covert surveillance will not be excluded unless the test of unfairness is met.

5. Definitions

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

5.2 '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))

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

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

- 5.4 'Surveillance' includes monitoring, observing, listening, with or without the assistance of a surveillance device, and includes recording of any information obtained.
- 5.5 Private information includes, and possibly goes beyond, information relating to a persons private or family life, and aspects of business and professional life.
- 5.6 '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. **The Council may not authorise such surveillance.**
- 5.7 'Authorising officer' in the case of local authorities these are specified as the Deputy Chief Executive (and more senior officers), Heads of Service, Service Managers or equivalent, responsible for the management of an investigation (see Regulation of Investigatory Powers (Directed Surveillance and Covert Human Intelligence Sources) Order 2010 (SI 2010 No.521) As amended (from 1st November 2012) by the Regulation of Investigatory Powers (Directed Surveillance and Covert Human Intelligence Sources (Amendment) Order 2012 No. 1500.
- 5.8 'Senior Responsible Officer' is responsible for:
- the integrity of the process in place within the public authority for the management of CHIS;
 - compliance with Part II of the Act and with the Codes;
 - oversight of the reporting of errors to the relevant oversight Commissioner and the identification of both the cause(s) of errors and the implementation of processes to minimise repetition of errors;
 - engagement with the **IPCOOSC** inspectors when they conduct their inspections, where applicable; and
 - where necessary, oversight of the implementation of post-inspection action plans approved by the relevant oversight Commissioner.

Within local authorities, the Senior Responsible Officer should be a member of the corporate leadership team and should be responsible for ensuring that all authorising officers are of an appropriate standard in light of any recommendations in the inspection reports prepared by the Office of the Surveillance Commissioner. Where an inspection report highlights concerns about the standards of authorising officers, this individual will be responsible for ensuring the concerns are addressed. **See Appendix E.**

- 5.9 'RIPA Monitoring Officer' is responsible for:
- Maintaining the central record and collation of documents,
 - Day to day oversight of the RIPA process
 - Organising training in RIPA, and
 - Raising awareness of RIPA within the Council

6. When does RIPA apply?

- 6.1 RIPA applies where the directed covert surveillance of an individual or group of individuals, or the use of a CHIS is necessary for the purpose of preventing or detecting crime, (see below).
- 6.2 The Council can only authorise **Directed Surveillance** to prevent and detect a criminal offence if it is punishable, whether on summary conviction or indictment, by a period of imprisonment of at least six months, or would constitute an offence under:
- (a) Section 146 Licensing Act 2003 (sale of alcohol to children)
 - (b) Section 147 Licensing Act 2003 (allowing the sale of alcohol to children)
 - (c) Section 147a 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 eighteen)

6.3 CCTV

The normal use of CCTV is not usually covert because members of the public are informed by signs that such equipment is in operation. However, authorisation should be sought where it is intended to use CCTV in a covert and pre-planned manner as part of a specific investigation or operation, for the surveillance of a specific person or group of people. Equally a request, say by the police, to track particular individuals via CCTV recordings may require authorisation (from the police).

6.4 COVERT SURVEILLANCE OF SOCIAL NETWORKING SITES

6.4.1 The use of the internet and, in particular, social networking sites, can provide useful information for Council staff carrying out investigations. These investigations may relate to the various enforcement roles within the Council for example Planning, Licensing or Environmental Health but will equally apply to some non-enforcement teams, such as debt collection or Housing. The use of the internet and social networking sites may potentially fall within the definition of covert directed surveillance. This is likely to result in the breaching of an individual's Article 8 rights under the Human Rights Act (the right to privacy).

6.4.2 In using social media for the gathering of evidence:

- officers must not 'friend' individuals on social networks
- officers should not use their own private accounts to view the social networking accounts of other individuals
- officers viewing an individual's profile on a social networking site should do so only once in order to obtain evidence to support or refute their investigation

Formatted: Underline

Formatted: Outline numbered + Level: 2 + Numbering Style: 1, 2, 3, ... + Start at: 1 + Alignment: Left + Aligned at: 0 cm + Indent at: 1.27 cm

Formatted: Indent: Left: 1.27 cm

Formatted: Outline numbered + Level: 3 + Numbering Style: 1, 2, 3, ... + Start at: 1 + Alignment: Left + Aligned at: 0 cm + Indent at: 1.27 cm

Formatted: Indent: Left: 1.27 cm

Formatted: Indent: First line: 1.27 cm

Formatted: Indent: Left: 1.27 cm

- further viewing of open profiles on social networking sites to gather evidence or to monitor an individual's status, must only take place once RIPA authorisation has been granted and approved by a Magistrate
- officers should be aware that it may not be possible to verify the accuracy of information on social networking sites and, if such information is to be used as evidence, steps must be taken to ensure its validity.

6.4.3 If an allegation is received or, as part of an investigation into an individual, it is necessary to view their social networking site, officers may access the main page of the individual's profile once in order to take an initial view as to whether there is any substance to the allegation or matter being investigated. The initial viewing must be reasonable, for example, it would not be reasonable to spend any significant amount of time searching through various pages of the individual's profile or to print out several pages just in case they may reveal something useful.

Formatted: Outline numbered + Level: 3 + Numbering Style: 1, 2, 3, ... + Start at: 3 + Alignment: Left + Aligned at: 0 cm + Indent at: 1.27 cm

6.4.4 In some cases, where, for example, a link to a site is provided by a complainant, it may be relevant for the receiving officer to view the link before passing it onto the investigating officer to also view. This would count as one viewing. However, it would not be reasonable for each officer in a team to view the site in turn so that they may each gather some information.

Formatted: Indent: Left: 1.27 cm

Formatted: Outline numbered + Level: 3 + Numbering Style: 1, 2, 3, ... + Start at: 3 + Alignment: Left + Aligned at: 0 cm + Indent at: 1.27 cm

6.4.5 If there is a need to monitor an individual's social networking site, authorisation must be obtained. If the offence being investigated falls under RIPA, a formal RIPA application must be completed, authorised by an Authorising Officer and then approved by a Magistrate.

Formatted: List Paragraph, Left, No bullets or numbering

Formatted: Outline numbered + Level: 3 + Numbering Style: 1, 2, 3, ... + Start at: 3 + Alignment: Left + Aligned at: 0 cm + Indent at: 1.27 cm

6.4.6 This is a useful tool and an authorisation for directed surveillance need only be sought where staff are 'systematically collecting and recording information about a particular person or group'. Further guidance regarding the factors to be considered can be found at paragraph 3.16 of the Code of Practice.

Formatted: List Paragraph, Left, No bullets or numbering

Formatted: Outline numbered + Level: 3 + Numbering Style: 1, 2, 3, ... + Start at: 3 + Alignment: Left + Aligned at: 0 cm + Indent at: 1.27 cm

Formatted: Indent: Left: 0 cm

7. Covert Human Intelligence Source

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

- 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)
- covertly uses such a relationship to obtain information or provide access to any information to another person; or
- covertly discloses information obtained by the use of such a relationship or as a consequence of the existence of such a relationship

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

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

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

- 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
- a relationship is used covertly, and information obtained as mentioned in- 7 (c) above and is disclosed covertly, if, and only if it is used or as the case may be, disclosed in a manner that is calculated to ensure that one of the parties to the relationship is unaware of the use or disclosure in question.

7.2 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 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.

7.3 Juvenile Sources

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 subject to at least monthly reviews to ensure that it is maintained for no longer than necessary. The Regulation of Investigatory Powers (Juvenile) Order 2000 SI as amended by the Regulation of Investigatory Powers (Juveniles) (Amendment) Order 2018 No 2793 contains special provisions which must be adhered to in respect of juvenile sources. This can only be authorised by the Chief Executive~~Director of Business~~.

7.4 Vulnerable Individuals

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 or illness and who 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. Again this can only be authorised by the Chief Executive~~Director of Business~~.

7.5 Legal Advice

Please consult the Monitoring Officer~~Director of Business~~ before taking any practical steps to authorise a CHIS.

7.6 Handler and Controller

There needs to be in place arrangements for the proper oversight and management of CHIS, including appointing individual officers as defined in section 29(5)(a) and (b) of the 2000 Act for each CHIS.

The Handler has day to day responsibility for:

- Dealing with the CHIS on behalf of the authority;
- Directing the day to day activities of the CHIS
- Recording the information supplied by the CHIS, and
- Monitoring the CHIS's security and welfare.

The Handler will usually be a rank or position below that of the authorising officer.

The Controller will normally be responsible for the management and supervision of the "handler" and general oversight of the use of the CHIS

8. **Authorisation Process and Oversight Arrangements**

8.1 Applications for directed surveillance

All application forms (**see Appendix A**) must be fully completed with the required details to enable the Authorising Officer to make an informed decision. Sections 12 and 13 of the form must be completed by the Authorising Officer.

An authorisation under the 2000 Act will only ensure that there is a justifiable interference with an individual's Article 8 rights if it is **necessary** and **proportionate** for these activities to take place. Therefore, the grant of authorisation should indicate that consideration has been given to these points and no authorisation shall be granted unless the Authorising Officer is satisfied that the investigation is:

- **necessary** for either the prevention or detection of crime, involving a criminal offence punishable whether by summary or on indictment by a maximum sentence of at least six months imprisonment or related to the underage sale of alcohol or tobacco (see paragraph 6.2 for offences). Covert surveillance cannot be said to be necessary if the desired information can reasonably be obtained by overt means

- **proportionate** - if the activities are necessary, the person granting the authorisation must believe that they are **proportionate** to what is sought to be achieved by carrying them out. This involves balancing the intrusiveness of the activity on the target and others (see 8.4 Collateral intrusion) that might be affected by it against the need for the activity in operational terms.

The method of surveillance proposed must not be **excessive** in relation to the seriousness of the matter under investigation. It must be the method which is the **least invasive** of the target's privacy.

The activity will not be proportionate if it is excessive in the circumstances of the case or if the information which is sought could reasonably be obtained by other less intrusive means. All such activity should be carefully managed to meet the objective in question and must not be arbitrary or unfair.

The **privacy** of innocent members of the public must be respected and collateral intrusion minimised – see 8.4 below.

It must be at an **appropriate** level (i.e. not excessive) and no other form of investigation would be appropriate.

8.2 Necessity

The Authorising Officer must be satisfied that the use of covert surveillance is necessary for one of the purposes specified in Section 28(3) of RIPA. In order to be satisfied, the conduct that it is aimed to prevent or detect must be identified and clearly described, particularly if it is questionable whether the serious crime criteria are met.

8.3 Proportionality

Proportionality is not only about balancing the effectiveness of covert methods over overt methods but of explaining why a particular covert method, technique or tactic is the least intrusive. It is insufficient to make a simple assertion or to say that the `seriousness` of the crime justifies any or every method available. It may be unacceptable to advance lack of resources or a potential cost saving as sufficient ground to use technological solutions which can be more intrusive than a human being. This critical judgment can only be reached once all aspects of an authorisation have been fully considered. It will be helpful to consider the following elements:

- (i) That the proposed covert surveillance is proportional to the mischief under investigation;
- (ii) That is proportional to the degree of anticipated intrusion on the target and others, and
- (iii) It is the only option, other overt means having been considered and discounted.

The following elements of proportionality should therefore be considered:

- balancing the size and scope of the operation against the gravity and extent of the perceived mischief,
- explaining how and why the methods to be adopted will cause the least possible intrusion on the target and others,
- that the activity is an appropriate use of the legislation and the only reasonable way, having considered all others, of obtaining the necessary result, and
- providing evidence of other methods considered and why they were not implemented

The Authorising Officer should set out, in ~~their~~ own words, "*I am satisfied*" and "*I believe*" why ~~they are~~ satisfied or why ~~they believe~~ the activity is necessary and proportionate

8.4 Collateral intrusion

The privacy rights of members of the public who are not the subject of the investigation, must be minimised and the surveillance must be carefully controlled so as to respect those rights.

The Authorising Officer must also take into account the risk of '**collateral intrusion**' i.e. intrusion on, or interference with, the privacy of persons other than the subject of the investigation, particularly where there are special sensitivities e.g. premises used by lawyers, MPs, doctors or priests e.g. for any form of medical or professional counselling or therapy. The application must include an **assessment** of any risk of collateral intrusion for this purpose.

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

Those carrying out the investigation must inform the Authorising Officer of any unexpected interference with the privacy of individuals who are not covered by the authorisation as soon as these become apparent.

Where such collateral intrusion is unavoidable, the activities may still be authorised, provided the intrusion is considered proportionate to what is sought to be achieved.

8.5 Special consideration in respect of confidential information

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

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

8.6 Legal privilege

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

If in doubt, the advice of Legal Services should be sought in respect of any issues in this area.

8.7 Confidential personal information

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**.

8.8 Confidential journalistic material

This is material acquired or created for the purposes of journalism and held subject to an undertaking to hold it in confidence. It should be noted that matters considered to be confidential under RIPA may not necessarily be properly regarded as confidential under section 41 Freedom of Information Act.

Where confidential information as referred to in sections 8.4 to 8.5 is likely to be acquired, the surveillance may only be authorised by the ~~Chief Executive-Director of Business~~ and should only be authorised where there are exceptional and compelling circumstances.

8.9 Authorisations must be in writing.

The Regulation of Investigatory Powers (Directed Surveillance and Covert Human Intelligence Sources (Amendment) Order 2012 amended the 2010 Order - see the new 7A which states that the serious crime threshold of investigating criminal offences with a sentence of at least six months imprisonment and those offences related to the underage sale of alcohol and tobacco apply.

8.10 Notifications to Inspector/Commissioner

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

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

8.11 Applications for CHIS

The application is the same as for directed surveillance except that the serious crime threshold of investigating criminal offences with a sentence of at least six months 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.

There are additional requirements in s29(5) relating to responsibility for dealing with the source and maintenance of records relating to the source.

All application forms must be fully completed with the required details to enable the Authorising Officer to make an informed decision.

In addition to the requirements of RIPA, the duties set out in the Source Records Regulations (S.I.2000/2725) must also be observed.

Please consult the ~~Monitoring Officer~~~~Director of Business~~ before taking any practical steps to authorise a CHIS.

8.12 Judicial Approval of authorisations

Once the Authorising Officer has authorised the directed surveillance or CHIS, the Investigating Officer who completed the application form should contact Legal Services who will arrange a hearing at the appropriate Magistrates' Court. A member of the Legal Services Team will accompany the Investigating Officer to present the application for approval by a Justice of the Peace. The hearing is a legal proceeding and therefore, if not represented by Legal Services, local authority officers need to be formally designated to appear.

The Investigating Officer ~~or Authorising Officer~~ will provide the Justice of the Peace with a copy of the original authorisation or notice and the supporting documents setting out the case. This forms the basis of the application to the Justice of the Peace and should contain all information that is relied upon.

In addition, the Investigating Officer ~~or~~ will provide the Justice of the Peace with two copies of a partially completed judicial application/order form.

The hearing must be in private (unless the Court otherwise directs) and the officer will be sworn in and present evidence as required by the Justice of the Peace. Any such evidence should be limited to the information in the authorisation. It is not sufficient for the local authority to provide oral evidence where this is not reflected or supported in the papers provided.

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

The Order Section of the above mentioned form will be completed by the Justice of the Peace and will be the official record of his/her decision. The Council will need to retain a copy of the form after it has been signed by the Justice of the Peace.

The Justice of the Peace can:

- (a) approve the Grant of or renewal of an Authorisation or Notice, which means the authorisation will then be effective.
- (b) refuse to approve the Grant of Authorisation or Notice, which means that 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 Authorisation or renewal and quash the original authorisation. The Court cannot exercise its power to quash the authorisation unless the applicant has at least two business days from the date of the refusal to make representations.

Appeals

The Council may only appeal a Justice of the Peace's decision on a point of law by making an application for judicial review in the High Court. The Investigatory Powers Tribunal (IPT) will continue to investigate complaints by individuals about the use of the RIPA techniques by public bodies, including local authorities. If, following a complaint to them, the IPT finds fault with a RIPA authorisation or notice it has the power to quash the Justice of the Peace's order which approved the grant or renewal of the authorisation or notice.

8.13 Working in partnership with the police

Authorisation can be granted in situations where the police rather than the 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.

9. 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.
- If renewed the authorisation shall cease to have effect 3 months from the expiry of the original authorisation.
- An authorisation for **CHIS** shall cease to have effect (unless renewed) 12 months from the date the Justice of the Peace approves the grant or renewal (save for a Juvenile CHIS where the authorisation will have effect for 4 months with at least monthly reviews).

This does not mean that the authorisation should be given for the whole period so that it lapses at the end of this time. The Authorising Officer, in accordance with s45 of the Act, must cancel each authorisation as soon as that officer decides that the surveillance should be discontinued. Authorisations should continue for the minimum period reasonable for the purpose they are given and in any event will not last longer than 3 months.

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 any 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 instructions to cease surveillance should be retained and kept with the cancellation form.

10. Reviews

The Authorising Officer should review all authorisations at intervals determined by him/her. This should be as often as necessary and practicable. **The reviews should be recorded.**

If the directed surveillance authorisation provides for the surveillance of unidentified individuals whose identity is later established, the terms of the authorisation should be refined at review to include the identity of these individuals.

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

11. Renewals

If for any reason a Review is not carried out on time the authorisation may be cancelled. Notice of this cancellation must be given to the Authorising Officer immediately.

Any Authorised 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 the original authorisation was approved. The process already outlined in section 8 above should be followed.

A CHIS authorisation must be thoroughly reviewed before it is renewed.

12. Central Register of authorisations

12.1 The Council 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 Authorising Officer;
- 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 together with supporting documentation submitted when the renewal was requested;
- the date and time when any instruction to cease surveillance was given;
- the date and time when any instruction was given by the Authorising Officer;

12.2. To comply with section 12.1, the ~~Monitoring Officer~~~~Director of Business~~ will hold the Central Register of all authorisations issued by an officer of the Council. A copy of every authorisation, renewal and cancellation issued should be lodged immediately with the ~~Monitoring Officer~~~~Director of Business~~ in an envelope marked "Private and Confidential".

Any original authorisations and renewals taken to the Magistrates' Court should be retained by the Council because the Court only keep copies of the authorisations or renewals.

12.3. The Council must also maintain a centrally retrievable record of the following information:

- type of authorisation
- date the authorisation was given
- date the Approval Order was given by the Justice of the Peace.
- name and rank/grade of the authorising officer
- confidential information
- self-authorisations
- unique reference number of the investigation/operation
- title (including brief description and names of the subjects) of the investigation/operation;
- reviews
- details of renewal
- dates of any Approval Order for renewal given by the Justice of the Peace.
- whether the investigation/operation is likely to result in obtaining confidential information
- date of cancellation

These records will be retained for at least **3 years** and will be available for inspection by the IPCO, Office of Surveillance Commissioners.

13. Retention of records

The Council must ensure that arrangements are in place for the secure handling, storage and destruction of material obtained through the use of directed surveillance in accordance with the relevant Code of Practice. The Authorising Officers, through their relevant Data Controller, must ensure compliance with the appropriate data protection requirements under the Data Protection Act 20181998 and any relevant Codes of Practice relating to the handling and storage of material.

The Central Register of Authorisations will be kept securely in a locked cabinet in the Legal Services department.

14. Complaints procedure

- 14.1 The Council will maintain the standards set out in this guidance and the Codes of Practice. The Investigatory Powers Commissioner Chief Surveillance Commissioner has responsibility for monitoring and reviewing the way the Council exercises the powers and duties conferred by RIPA.
- 14.2 Contravention of the Data Protection Act 20181998 may be reported to the Information Commissioner. Before making such a reference, a complaint concerning a breach of this guidance should be made using the Council's own internal complaints procedure.

RIPA GUIDANCE – PART II
ACQUISITION AND DISCLOSURE OF
COMMUNICATIONS DATA

Introduction

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

A link to the Home Office Code of Practice – Acquisitions and Disclosure of Communications data is at Appendix G

The Protection of Freedoms Act 2012 made changes to the provisions under the Regulation of Investigatory Powers Act 2000 requiring the need for a local authority to seek judicial approval of the grant or renewal of an authorisation or of the giving or renewal of a notice.

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

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

The purpose and effect of the procedure is the same i.e. to ensure proper consideration is given to permitting such investigations and to provide protection against a human rights challenge.

The Authorising Officer is called a 'Designated Person'.

1. What is `Communication Data` ?

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

Traffic data - where a communication was made from, to whom and when
Service data – use made of service e.g. Itemised telephone records
Subscriber data – information held or obtained by operator on person they provide a service to.

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

2. Application Forms

The application form should be completed via the National Anti- fraud Network website at www.nafn.gov.uk. The National Anti-fraud Network SPoC Service (acting as SPoC for the Council), will assess and quality control the application. If it meets the legal threshold for obtaining communications data, the SPoC will post it on the website for approval by the appropriate Designated Person.

This procedure necessitates the applicant to be registered with the National Anti-fraud Network prior to making the application. For details on how to do this the applicant should visit www.nafn.gov.uk.

If rejected, by the Designated Person or the SPoC, the SPoC will retain the application and inform the applicant in writing of the reason(s) for its rejection. Comprehensive guidance on the application process is also available via the National Anti-fraud Network website at www.nafn.gov.uk

3. Authorisations

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

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

- i) it is **necessary** for any of the purposes set out in Section 22(2) of the Act. (NB the Council can only authorise for the purpose set out in Section 22 (2) (b) which is the purpose of preventing or detecting crime or preventing disorder); and
- ii) it is **proportionate** to what is sought to be achieved by the acquisition of such data (in accordance with Section 22(5) the Act)

Consideration must also be given to the possibility of collateral intrusion.

Once a Designated Person has decided to grant an authorisation or a notice is to given there are two methods:

- 1) By authorisation of some person in the same relevant public authority as the Designated Person, whereby the relevant public authority collects the data itself (Section 22(3) the Act). This may be appropriate in the following circumstances:
 - the postal or telecommunications operator is not capable of collecting or retrieving the communications data,
 - it is believed the investigation may be prejudiced if the postal or telecommunications operator is asked to collect the data itself,
 - there is a prior agreement in place between the relevant public authority and the postal or telecommunications operator as to the appropriate mechanisms for the disclosure of communications data,

- 2) By notice to the holder of the data to be acquired (Section 22(4)) which requires the operator to collect or retrieve the data. Disclosure may only be required to either the Designated Person or the SPOC.

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.

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

There are standard forms for authorisations and notice which are available using the link provided at Appendix F.

4. Oral Authority

The Council is not permitted to apply or approve orally.

5. Duration

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

6. Renewal and Cancellation

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

The code requires that all authorisations and notices should be cancelled by the Designated Person who issued it as soon as it is no longer necessary, or the conduct is no longer proportionate to what is sought to be achieved. The relevant postal or telecommunications operator should be informed of the cancellation of a notice.

7. Retention of Records

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

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

A record must be kept of:-

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

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

Communications data, and all copies, extracts and summaries of it, must be handled and stored securely and the requirements of the Data Protection Act ~~2018~~1998 must be observed.

The ~~Monitoring Officer~~~~Director of Business~~ will maintain a centrally retrievable register.

10. Oversight and Complaints

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

The Act also establishes an Independent Tribunal to investigate and decide any case within its jurisdiction.

REGULATION OF INVESTIGATORY POWERS ACT
2000 (RIPA)

APPENDIX A

Directed Surveillance and CHIS Forms

<S:\General Folder\RIPA\APPENDIX 1 - DS FORM.doc>

<S:\General Folder\RIPA\APPENDIX 2 - DIRECTED SURVEILLANCE review.doc>

<S:\General Folder\RIPA\APPENDIX 3 - DIRECTED SURVEILLANCE renewal.doc>

<S:\General Folder\RIPA\APPENDIX 4 - DIRECTED SURVEILLANCE cancellation.doc>

<S:\General Folder\RIPA\APPENDIX 5 - CHIS form.doc>

<S:\General Folder\RIPA\APPENDIX 6 - DIRECTED SURVEILLANCE review.doc>

<S:\General Folder\RIPA\APPENDIX 7 - CHIS RENEWAL FORM.doc>

<S:\General Folder\RIPA\APPENDIX 8 - CHIS CANCELLATION FORM.doc>

<S:\General Folder\RIPA\APPENDIX 9 - DS FORM with notes.doc>

<S:\General Folder\RIPA\APPENDIX 10 - Surveillance Risk Assess Pro Forma.doc>

<S:\General Folder\RIPA\APPENDIX 11 CHANGE OF CIRCUMSTANCES.doc>

<S:\General Folder\RIPA\APPENDIX 12 - Surveillance Control Matrix.doc>

REGULATION OF INVESTIGATORY POWERS ACT
2000 (RIPA)

APPENDIX B

Home Office Guidance to Local Authorities in
England
and Wales on the judicial approval process for
RIPA
and the crime threshold for directed surveillance

<https://www.gov.uk/government/publications/changes-to-local-authority-use-of-ripa>

REGULATION OF INVESTIGATORY POWERS ACT
2000 (RIPA)

APPENDIX C

Home Office guidance for Magistrates` Courts
in
England and Wales for a local authority application
seeking an order approving the grant or renewal of
a RIPA authorisation or notice

<https://www.gov.uk/government/publications/changes-to-local-authority-use-of-ripa>

REGULATION OF INVESTIGATORY POWERS ACT
2000 (RIPA)

APPENDIX D

Home Office - Codes of Practice – Covert
Surveillance and Property Interference and Covert
Human Intelligence Sources

<https://www.gov.uk/government/collections/ripa-codes>

<https://www.gov.uk/government/publications/code-of-practice-for-covert-surveillance-and-property-interference>

https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/97960/code-of-practice-covert.pdf

https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/276013/CovertHumanIntelligenceSources.pdf

REGULATION OF INVESTIGATORY POWERS ACT
2000 (RIPA)

APPENDIX E

AUTHORISING OFFICERS

~~Legal Services Manager~~

~~Head of Health, Housing and Regeneration~~

~~Director of Communities~~

~~Director of Economic Development~~

~~**Chief Executive**~~ ~~**Director of Business**~~ in the event that there is a possibility of confidential information being obtained as highlighted in 8.4 and 8.5 of this Policy.

SENIOR RESPONSIBLE OFFICER

~~**Director of Business**~~ ~~**Head of Legal (Monitoring Officer)**~~

Formatted: Font: 12 pt

Formatted: Normal, Left

REGULATION OF INVESTIGATORY POWERS ACT
2000 (RIPA)

APPENDIX F

Forms - Communications Data

www.nafn.gov.uk

<https://www.gov.uk/government/collections/ripa-forms--2>

REGULATION OF INVESTIGATORY POWERS ACT
2000 (RIPA)

APPENDIX G

Home Office - Codes of Practice - Acquisition and
Disclosure of Communications Data

<https://www.gov.uk/government/publications/code-of-practice-for-the-acquisition-and-disclosure-of-communications-data>



Investigatory Powers
Commissioner's Office

PO Box 29105, London
SW1V 1ZU

Mr. Neil Shaw
Chief Executive
Rossendale Borough Council
The Business Centre
Futures Park
Bacup
Rossendale
OL13 0BB

17 February 2021

Dear Mr. Shaw,

IPCO Surveillance and CHIS Inspection of Rossendale Borough Council

Please be aware that IPCO is not a “public authority” for the purpose of the Freedom of Information Act (FOIA) and therefore falls outside the reach of the FOIA. It is appreciated that local authorities are subject to the FOIA and that they may receive requests for disclosure of our reports. In the first instance the SRO should bring the matter to the attention of the IPCO Data Protection Officer (at: info@ipco.org.uk), before making any disclosure. This is also the case if you wish to make the content of this letter publicly available.

Rossendale Borough Council was recently the subject of a remote inspection by one of my Inspectors, Mr Graham Wright, who looked at your use of powers and procedures in relation to directed surveillance and CHIS. This was facilitated through Clare Birtwistle (Head of Legal and Senior Responsible Officer for RIPA) who provided information during discussion on 21st January 2021. This discussion related to the Council's current usage of the powers under RIPA, the response to the previous inspection in 2018, and your response to my letter of September 2020 regarding Data Assurance. Ms Birtwistle provided further information in relation to these matters recently.

The information provided has demonstrated a level of compliance that removes, for the present, the requirement for a physical inspection.

The previous recommendations from the 2018 inspection have all been adequately discharged. The main RIPA Policy document has been suitably amended (for more details see below); reporting to Elected Members on the Overview and Scrutiny Committee now occurs; and the Senior Responsible Officer is now sufficiently independent from the appointed authorising officers.

My Inspector has reviewed your Council's RIPA Policy. It is in many ways an accurate and useful document for applicants, authorising officers and anyone considering carrying out covert activity. It covers use of covert surveillance, CHIS and requests for Communications Data, which is done via the National Anti-Fraud Network. The document is currently in draft form and will be submitted to the Overview and Scrutiny Committee pending any comments from this inspection. In that regard Mr. Wright makes the following comments:

1. In relation to the matter of online covert activity, you have now incorporated a substantial section of advice. However, it needs to be made clear to staff that this is a useful tool and an authorisation for directed surveillance need only be sought where staff are 'systematically collecting and recording information about a particular person or group'¹. Further guidance regarding the factors to be considered can be found at paragraph 3.16 of the Code of Practice.
2. Paragraph 7.3 of the policy refers to juvenile CHIS and states that an authorisation has a duration of one month. This is incorrect. The duration is four months, and subject to at least monthly reviews. (It is accepted that the likelihood of such an authorisation being granted is extremely low, but the comment is made for the sake of accuracy.)

Although your Council has not exercised its powers since October 2012, the SRO was reminded of the importance of ensuring that the designated authorising officers maintain their level of training. Mr Wright was informed that training with relevant officers is undertaken on an *ad hoc* basis to ensure they continue to understand the requirements of RIPA. There have been no new investigating officers appointed for some time and they have all received appropriate training either with the Council, or with the police as their former employer. New Directors and the Chief Executive are booked onto an external training session in April 2021 which the SRO will attend also. There is also a training package on your internal training system, Learning Pool, which all staff can access at any time. An email to staff will be circulated to remind them of the courses available on the system and to undertake the RIPA course as a refresher.

As I have referred to above, the monitoring of social media and the internet can offer initial investigative leads and assist with your enforcement or other responsibilities, but it is important to ensure that such resources as these are used in a controlled, auditable, and well understood manner. The Home Office Covert Surveillance and Property Interference Code of Practice provides some helpful advice on this point. Your amended policy document now contains more suitable guidance and advice to staff with regards to how this should be used in a compliant manner.

In relation to the matter of the correct handling of material acquired by covert activity, or Communications Data, your Council is drawing up an action plan in response to the letter I sent to you in this regard in September 2020, and in particular the six action points at the conclusion of my letter. A review of the Council's retention and destruction policy has already taken place, and also the disposal of any data held under any previous authorisations.

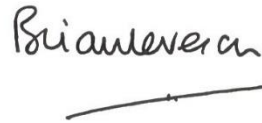
In conclusion, it must be emphasised that although your Council has not exercised its RIPA powers since 2012 it is vital that the relevant staff are appropriately trained should the need to authorise covert activity arise. It is also important that officers engaged in investigatory areas where RIPA considerations are not so immediately apparent, maintain their levels of knowledge and know whom to approach for guidance. The SRO has given assurances to the Inspector that the integrity of your Council's processes and governance procedures will be maintained to ensure that high standards of compliance with the Act and relevant codes of practice are achieved.

I hope that this telephone-based inspection has proved to be a worthwhile exercise. My Office is available to you should you have any queries following the recent inspection, or at any point in the future. Contact details are provided at the foot of this letter.

¹ Covert Surveillance Code of Practice paragraph 3.15

I shall be grateful if you would acknowledge receipt of this letter within two months.

Yours sincerely,

A handwritten signature in black ink that reads "Brian Leveson". The signature is written in a cursive style and is positioned above a horizontal line.

The Rt. Hon. Sir Brian Leveson
The Investigatory Powers Commissioner