HYNDBURN

The place to be

an excellent council

REGULATION OF INVESTIGATORY POWERS ACT 2000 (as amended by the Protection of Freedoms Act 2012)

CORPORATE POLICY AND AUTHORISATION PROCEDURES

Policy updated November 2018

REGULATION OF INVESTIGATORY POWERS ACT 2000

CORPORATE POLICY AND AUTHORISATION PROCEDURES

CONTENTS

		Page
Part 1	Introduction	3
Part 2	Legislative Background	5
Part 3	Surveillance	9
Part 4	Covert Human Intelligence Source	14
Part 5	Acquisition and Disclosure of Communications Data	17
Part 6	Obtaining a RIPA Authorisation	20
Part 7	Authorising Officers	25
Part 8	Working with/ through other agencies	28
Part 9	Record Management	29
Part 10	Training	31
	Annex – Codes of Practice	34

PART 1

INTRODUCTION

1.1 This Corporate Policy and Authorisation Procedures Document is based upon the requirements of The Regulation of Investigatory Powers Act 2000 (RIPA) (as amended by the Protection of Freedoms Act 2012) ,Statutory Instruments, the Codes of Practice issued by the Home Office and the advice of The Office of the Investigatory Powers Commissioners Office (IPCO)

1.2 Hyndburn Borough Council takes it statutory responsibilities seriously and will at all times act in accordance with the law. In particular it will take all necessary and proportionate action that may be required in order to ensure compliance with the provisions of RIPA and the Human Rights Act 1998.

1.3 The Executive Director, Legal and Democratic Services who has been appointed as the Senior Responsible Officer for the purposes of RIPA , is authorised to keep this Policy and Procedures Document under review and will amend, delete, add or substitute any of its provisions to such extent as may be necessary to keep it current.

1.4 The authoritative position on RIPA is the Act itself, secondary legislation made thereunder, the Codes of Practice and any relevant case law on their interpretation and application. This policy document incorporates the Guidance and Codes of Practice referred to at the Annex so it is especially important that every officer exercising a power or performing a function relating to RIPA must in so doing have specific regard to any relevant Code of Practice. Appropriate training will be given to officers undertaking any functions pursuant to RIPA.

1.5 If an officer is uncertain about any aspect of RIPA or anything contained in this document they must seek the advice of the Executive Director, Legal and Democratic Services.

1.6 In terms of monitoring e mails and Internet usage it is important to recognise the interplay and overlaps between RIPA and the Council's e mail and internet usage policies, the Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000, (as amended by The Privacy and Electronic Communications (EC Directive) Regulations) 2003 and the Data Protection Act 2018.

1.7 In the event of the Executive Director, Legal and Democratic Services being absent or the post being vacant the Council's Chief Executive will nominate an officer to exercise his/ her duties under RIPA.

PART 2

LEGISLATIVE BACKGROUND

2.1 The Human Rights Act 1998 (HRA) incorporated into the UK legal system a series of rights created by the European Convention for the Protection of Human Rights and Fundamental Freedoms 1950 (ECHR).

2.2 Article 8 of the Convention states that ;
"Everyone has the right to respect for his private and family life, his home and his correspondence.
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 protection of the rights and freedoms of others"

2.3 It should be noted that the rights conferred by Article 8 are qualified so it is still possible for a public authority to infringe those rights providing the following criteria are satisfied;

It is done in accordance with the law:

It is necessary:

It is proportionate:

2.4 The surveillance of an individual or the use of a covert informant by or on behalf of a public body will constitute an infringement of the Human Rights Act 1998 (i.e. interference with right to privacy contrary to article 8 ECHR) **unless** these three criteria are satisfied.

2.5 If the three criteria are not met, any breach of the HRA may give rise to a civil claim against the authority by the person whose rights have been infringed (Section 7 HRA)

2.6 Contravention of the HRA may also render evidence inadmissible in a criminal trial if it results in unfairness to the accused.

2.7 A breach of the HRA by Local Authority can in addition lead to a complaint being lodged with the Ombudsman.

2.8 **In accordance with the law.** As there was no law in the UK to provide explicit protection from an intrusion into privacy RIPA was enacted to provide legal authority for such intrusion in appropriate cases.

2.9 **It is necessary.** Necessity means that in the particular circumstances of each enquiry there is no reasonably available overt method of obtaining the information that is being sought. This test will have to be applied to each case on its own merits but if there is a reasonable alternative to covert surveillance then the necessity test will probably not be satisfied.

2.10 **It is proportionate.** Judging proportionality will probably involve four considerations:

- balancing the size and scope of the proposed activity against the gravity and extent of the perceived crime of offence;
- explaining how and why the methods to be adopted will cause the least possible intrusion on the subject and others;
- 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;
- evidencing, as far as reasonably practicable, what other methods had been considered and why they were not implemented.

2.11 The provisions of RIPA that apply to Local Authorities provide a regulatory framework that permits;

The use of Directed Surveillance (Part 3)
The Use of Covert Human Intelligence Sources (CHIS) (Part 4)
The Acquisition and Disclosure of Communications Data (Part 5)

2.12 RIPA does not;

make unlawful anything that is otherwise lawful
impose any new statutory duties (N.B. but see paragraphs 2.5 –2.7 on the possible consequences of non- compliance)
prejudice or dis-apply any existing powers available to the Council to obtain information by any means not involving conduct that is governed by RIPA. For example it does not affect the Council's current powers to obtain information from the DVLA or the Land Registry.

2.13 On the 1st November 2012 RIPA was amended by sections 37 and 38 of the Protection of Freedoms Act 2012 which combined introduced legal requirements that authorisations for the use of directed surveillance or CHIS and the authorisation or giving of notice for obtaining or disclosing communication data by Local Authorities can only take effect after an order approving the authorisation or notice has been granted by a Magistrate.

2.14 The use of directed surveillance by the Local Authorities was also restricted (with exceptions relating to the sale of alcohol and tobacco which are not enforced by the Council) with effect from the 1st November 2012 to the prevention or detection of crimes that attracted a penalty of imprisonment for 6 months or more . This threshold was imposed by The Regulation of Investigatory Powers (Directed Surveillance and Covert Human Intelligence Sources) (Amendment) Order 2012.

2.15 Through the application of authorisation procedures RIPA ensures that a balance is maintained between the public interest and the human rights of individuals. An additional safeguard is provided by the judicial scrutiny of the use of authorisations

2.16 If the RIPA procedures are followed correctly the conduct of an investigation will be deemed lawful for all purposes (section 27 RIPA). This protection extends to criminal and civil proceedings, Employment Tribunal hearings and a complaint to either the Local Government Ombudsman or the Investigatory Powers Tribunal. It therefore provides protection both for the Council and any officer who may have been involved in an investigation.

2.17 The use of the powers conferred by RIPA is subject to scrutiny by IPCO, which may carry out periodic inspections of the Council's practices and procedures. It is therefore essential that surveillance is always carried out in compliance with RIPA, the policies and codes of practice annexed to in this document and any advice or guidance that may be issued from time to time by the Executive Director, Legal and Democratic Services.

PART 3

SURVEILLANCE

3.1 "**Surveillance"** includes

monitoring, observing listening to persons, their movements, listening to their conversations or their other activities or communications;

recording anything monitored, observed or listened to in the course of surveillance; and

surveillance by or with the assistance of a surveillance device.

Surveillance can be either overt or covert.

3.2 **Overt Surveillance**

Most of the surveillance undertaken by the Council will be done overtly – there will be nothing secretive, clandestine or hidden about it. In many cases officers will be going about Council business openly (e.g. a routine inspection by an Environmental Health Officer) or will have notified the subject of the investigation that they are likely to be under surveillance. In the latter case officers need to be particularly alert to the possibility that the proposed surveillance may entail collateral intrusion into the lives and activities of persons other than the subject of the investigation (e.g. a visitor to premises). If there is the slightest possibility of collateral intrusion a RIPA authorisation should be obtained before any surveillance is carried out.

3.3 **Covert Surveillance**

Covert Surveillance is carried out in a manner calculated to ensure that the person who is the subject of the surveillance is unaware that it is taking place.

3.4 **Directed Surveillance**

Directed Surveillance is surveillance that is
covert but not intrusive surveillance; (see paragraph 3.6)

undertaken for the purpose of a specific investigation or operation.

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

not carried out as an immediate response to events which would otherwise make seeking authorisation under RIPA unreasonable (e.g. spotting something suspicious and continuing to observe it)

Private Information

This phrase is defined in RIPA section 26 (10) as including any information relating to a person's private or family life. The European Court of Human Rights has considered this definition and has found that private life is a broad term not susceptible to exhaustive definition. Aspects such as gender identification, name, sexual orientation and sexual life are important elements of the personal sphere protected by Article 8. The Article also protects a right to identity and personal development and the right to establish and develop relationships with other human beings and the outside world and it may include activities of a professional or business nature. There is therefore a zone of interaction of a person with others even in a public context, which may fall within the scope of "private life".

The fact that covert surveillance occurs in a public place or on business premises does not necessarily mean that it cannot result in the acquisition of private information about a person. Prolonged surveillance targeted on a single person will undoubtedly result in the

obtaining of private information about him/her and others that he / she comes into contact with or with whom they associate.

Similarly, although the overt use of CCTV cameras does not normally require authorisation if the camera is used for a particular purpose that involves the prolonged surveillance of a particular person, a RIPA authorisation will be required. The use of CCTV is dealt with in more detail at Part 8

3.6 **Intrusive Surveillance**

Intrusive Surveillance

Is covert

Relates to residential premises or vehicles and

Involves the presence of a person in the premises or in the vehicle or which is carried out by a surveillance device in the premises or vehicle. Surveillance equipment mounted outside the premises will not be intrusive unless the device consistently provides information of the same quality and detail as might be expected if it were in the premises or vehicle.

3.6 **Local Authorities <u>can</u> undertake directed surveillance but <u>cannot</u> carry out intrusive surveillance.**

3.7 **The Council will only carry out directed surveillance pursuant to a RIPA authorisation where the purpose of the investigation or operation is directed at preventing or detecting crime which is punishable by a maximum term of at least 6 months imprisonment.**

3.8 **Confidential Information**

RIPA does not provide for any special protection for confidential Information. Nevertheless, particular care should be taken in cases where the subject of the investigation or operation might reasonably expect a high degree of privacy, or where confidential information is involved. Confidential Information consists of matters subject to legal privilege, confidential personal information or confidential journalistic material. So for example, extra care should be taken where, through the use of surveillance, 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.

In cases where through the use of surveillance it is likely that knowledge of confidential information will be acquired the surveillance must be authorised by the Chief Executive as Head of the Paid Service (or in his absence by another authorised Chief Officer).

3.9 **Where a RIPA Authorisation is not Required**

In some situations surveillance does not constitute either intrusive or directed surveillance for the purposes of RIPA so no authorisation can be granted for that activity.

3.10 Examples of such surveillance activity include:

Covert surveillance by way of an immediate response to events:
Covert surveillance as part of general observation activities:
Covert surveillance not relating to specified grounds:
Overt use of CCTV systems. (this is governed by specific CCTV policies)

Covert Surveillance of Social Networking Sites

The Home Office revised code of practice (2018) on covert surveillance and property interference states that

"*The growth of the internet, and the extent of the information that is now available online, presents new opportunities for public authorities to view or gather information which may assist them in preventing or detecting crime or carrying out other statutory functions, as well as understanding and engaging with the public they serve. it is important that public authorities are able to make full and lawful use of this information for their statutory purposes. Much of it can be accessed without the need for RIPA authorisation; use of the internet prior to an investigation should not* ***normally engage privacy considerations. But if the study of an individual's online*** *presence becomes persistent, or where material obtained from any check is to be extracted and recorded and may engage privacy considerations, RIPA authorisations may need to be considered.*

The guidance then offers advice and illustrative examples of the use of RIPA in the context of on- line investigations. Reference should therefore be made to the Home Office Guidance when undertaking on line covert investigations to which RIPA applies.

PART 4

COVERT HUMAN INTELLIGENCE SOURCE (CHIS)

4.1 A person is a covert human intelligence source if

a) he establishes or maintains a personal or other relationship with a person for the covert purpose of facilitating the doing of anything falling within paragraph b) or c);
b) he covertly uses such a relationship to obtain information or to provide access to any information to another person; or
c) he covertly discloses information obtained by the use of such a relationship or as a consequence of the existence of such a relationship.

4.2 A member of the public who volunteers information to the Council may or may not a covert human intelligence source depending on the circumstances surrounding the acquisition of the information. Where information is received particularly repeat information about the same person consideration should be given, before using the information, to whether the informant is a CHIS to whom a duty of care is owed.

4.3 **The conduct or use of CHIS must be authorised in accordance with RIPA and approved by order of a Magistrate.**

Conduct of CHIS. This is establishing or maintaining a personal or other relationship with a person for the covert purpose of (or is incidental to) obtaining or passing on information

Use of a CHIS. This includes inducing, asking or assisting a person to engage in the conduct of a source or to obtain information by means of the conduct of such a source.

4.4 **Local Authorities can only authorise the conduct or use of CHIS for the purposes of preventing or detecting crime or of preventing disorder.**

4.5 Obtaining an authorisation under RIPA will only ensure that the authorised use or conduct of a source is a justifiable interference with an individual's rights under the Human Rights Act 1998 if it is necessary and proportionate for the source to be used. The use of a source will not be proportionate if it is excessive in the circumstances of the case or if the information that is sought could reasonably be obtained by other less intrusive means. An application for an authorisation should include an assessment of the risk of any collateral intrusion into the lives of those not directly connected with the operation.

4.6 **Juvenile Sources.**

Special safeguards apply to the use or conduct of juvenile sources (i.e. under 18 years of age). On no occasion can a child under 16 years of age be authorised to give information against his or her parents. Only the Chief Executive as Head of the Council's Paid Service should issue such authorisations as there are other requirements for such matters

4.7 **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 themselves or unable to protect themselves against significant harm or exploitation. A vulnerable individual will only be authorised as a CHIS in the most exceptional of circumstances. Only the Chief Executive as Head of the Council's Paid Service should issue such authorisations, as there are other requirements for such matters.

4.8 **Confidential Information**

RIPA does not provide any special protection for confidential information but particular care should be taken in cases where an

authorisation is likely to lead to the acquisition of matters subject to legal professional privilege, confidential information or confidential journalistic material. In cases where through the use or conduct of a source it is likely that confidential information will be acquired the authorization must be granted by the Chief Executive as Head of the Paid Service (or in his absence by an authorised Chief Officer)

4.9 **Anti-Social Behaviour**

Members of the public who report allegations of anti-social behaviour and are asked to keep a note of incidents will not normally be CHIS as they are not usually required to establish or maintain a covert relationship. However in some circumstances they may require a RIPA authorisation to undertake directed surveillance, for example using a video recorder. See Paragraph 4.2 above.

PART 5

ACQUISITION AND DISCLOURE OF COMMUNICATIONS DATA

5.1 The powers contained in Part 1 of Chapter 2 of RIPA permit Local Authorities to obtain information relating to the use of a postal service or telecommunications system. **It does not permit access to the content of the communication**

The Information can be obtained in two ways:-
by Authorisation or
by Notice

5.2 An authorisation permits the Local Authority to obtain the data itself. A notice would be given to the postal or telecommunications operator which is then obliged to provide the authority with the information stipulated in the notice.

5.3 **An authorisation or notice can only be obtained where it is necessary for the purpose of preventing or detecting crime or of preventing disorder. The authorisation of notice will not however take effect until approved by order of a Magistrate.**

Definition of Communications Data

any traffic data comprised in or attached to a communication (whether by the sender or otherwise) for the purposes of any postal service or telecommunications system by means of which it is being or may be transmitted; **(Traffic Data)**

any information which includes none of the contents of a communication (apart from information falling within above paragraph and is about the use made by any person of any postal service or telecommunications service or in connection with the provision to or use by any person of any telecommunications service or any port of a telecommunications system. (**Service Data)**

any information not falling within either of the above paragraphs that is held or obtained in relation to persons to whom he provides the service by a person providing a postal service or telecommunications service.(**Subscriber Data)**

Traffic Data in relation to communications means

any data identifying or purporting to identify, any person, apparatus or location to or from which the communication is or may be transmitted

any data identifying or selecting or purporting to identify or select apparatus through which, or by means of which the communication is or may be transmitted.

Any data comprising signals for the actuation of apparatus used for the purposes of a telecommunications system for effecting (in whole or in part) the transmission of any communication and

any data identifying the data or other data as data comprised in or attached to a particular communication.

But that expression includes data identifying a computer file or computer program access to which is obtained, or which is run by means of the communication to the extent only that the file or program is identified by reference to the apparatus in which it is stored.

Traffic Data therefore covers the sender and recipients of a communication; the location of a communication, online tracking of it; call detail records for specific calls, web browsing information (which sites have been visited and for how long) and postmarks and postal addresses.

Service Data covers connection records, timing and duration of calls, connection, re-connection and disconnection data, use of forwarding or re-direction services, additional telecommunications services and records of postal items.

Subscriber Data includes information on subscribers of e-mail and telephone accounts, account information, including payment details, addresses for installing and billing and abstract personal records such as sign up data

Local Authorities can only access Service and Subscriber Data. An authorisation will last for one month and should be renewed or cancelled as appropriate.

Where the statutory purpose is crime there is a serious crime threshold for the acquisition of service or traffic data. Subscriber data can still be acquired for any crime (where necessary and proportionate to do so).

A serious crime is

- An offence that is capable of attracting a prison sentence of 12 months or more.
- An offence by a person who is not an individual (i.e. a corporate body).
- An offence failing within the definition of serious crime in section 81(3) (b) of RIPA (i.e. where the conduct involves the use of violence, results in substantial financial gain or is by a large number of persons in pursuit of a common purpose).
- An offence which involves, as an integral part of it, the sending of a communication.
- An offence which involves, as an integral part of it, a breach of a person's privacy.

PART 6

OBTAINING A RIPA AUTHORISATION

6.1 Directed surveillance, the use of CHIS and the acquisition of communications data must be lawfully carried out in strict accordance with the terms of the relevant authorisation.

6.2 The Council will only very occasionally make use of CHIS so the applicant officer should consult the Executive Director, Legal and Democratic Services before making an application for a CHIS authorisation in order to ensure that the current statutory requirements and best practice are being observed.

6.3 Applications for authorisations and notices requesting communications data must be processed through the Council's Home Office accredited single point of contact. As the need to obtain such information will only very occasionally arise the applicant officer should contact the Executive Director Legal and Democratic Services before making an application in order to ensure that current statutory requirements and best practice are being observed.

6.4 **Making the Application**

Before making an application for an authorisation the requesting officer must;

read this policy document and the appropriate code of practice

determine whether the activity that they are proposing to conduct involves directed surveillance or the use of CHIS.

Assess whether the proposed activity is governed by RIPA.

If the proposed activity is governed by RIPA

Assess whether the activity is necessary and why.

Assess whether the activity is proportionate

If the activity could be conducted overtly or if a less intrusive option is available and practical use that option in preference to a RIPA authorisation.

Consideration should also be given to the possibility of collateral intrusion into the privacy of persons other than the subject of the operation. Steps must be taken whenever practicable to avoid or minimise (so far as may be possible) collateral intrusion. The likelihood of collateral intrusion will be a factor in assessing proportionality.

6.5 **The Application Forms**

The Home Office has published standard forms for the use by local authorities. These can be downloaded from the Home Office website.

If the applicant officer is unable to access this website the appropriate form can be obtained from the Executive Director Legal and Democratic Services.

Each operation/ investigation must be allocated a unique reference number (URN). This will comprise application No / year / department and should be entered on the form. The URN will be issued on application to the officer to whom this function has been delegated by the Executive Director Legal and Democratic Services and must be obtained before an application is completed.

Every box in the application form must be completed or marked n/a where it is not applicable.

Application Information – Best Practice

The following guidelines should be considered as best working practice with regard to all authorisations covered by this policy:

Applications should avoid any repetition of information;

Information contained in applications should be limited to that required by the relevant legislation;

An application should not require the sanction of any person in the Council other than the authorising officer;

Where it is forseen that other agencies will be involved in carrying out the surveillance, those agencies should be detailed in the application; Authorisations should not general be sought for activities already authorised following an application by the same or a different public authority.

The application should describe the nature of activity for which authorisation is being sought and the purpose of the investigation.

The application should also include
The reasons why the authorisation is necessary in the particular case and on the grounds under which it is made (i.e. for the purpose of preventing or detecting crime
The nature of the surveillance;
The identities, where known of the subjects of the surveillance;
A summary of the intelligence case;
An explanation of the information which it is desired to obtain as a result of the surveillance;
The details of any potential collateral intrusion and why that intrusion is justified;
The details of any confidential information that is likely to be obtained as a consequence of the surveillance;

The reasons why the surveillance is considered proportionate and what it seeks to achieve;

RIPA applications have a limited duration but do not automatically expire.

The application form must be reviewed on the date stated in the application form. Authorisations to carry out directed surveillance last for a maximum of **3 months**. Authorisations for CHIS last for a maximum period of **12 months**. Authorisations relating to communications data last **1 month.**

When a RIPA authorisation is reviewed the appropriate form should be completed

If a RIPA authorisation is no longer required the applicant officer must notify the authorising officer who granted the application who will cancel the application. There is a form for cancellation of an authorization. **A cancellation form must be completed in every case.**

If an investigation/ operation is likely to extend beyond the time limit applicable to a particular authorisation it must be renewed on the appropriate form.

The RIPA forms relating to every operation / investigation must be retained on the departmental RIPA file.

The application form once completed by the applicant officer must be submitted to an authorising officer together with a risk assessment. Each application must be considered on its own merits. In the Procedures and Guidance previously issued by the Office of Surveillance Commissioners applicants are advised that

"Template forms inevitably lead to, or at least give the appearance of minimal or no consideration of: (a) the nature and extent of the surveillance proposed and the justification for the use of the devices to be employed; (b) necessity; (c) proportionality; (d) collateral intrusion; and (e) what alternative methods have been considered. Template entries are therefore to be avoided or used with great care."

Once issued a copy or every RIPA form must be sent to the Executive Director, Legal and Democratic Services. The form should be in a sealed envelope marked "**Confidential RIPA forms"**

When a RIPA authorisation has been issued by an Authorising Officer it cannot be acted upon unless and until it has been approved by a Magistrate. The application for approval pursuant to the Protection of Freedoms Act 2012 will be made either by the Executive Director (Legal and Democratic Services) or the Legal Services Manager.

Guidance on the making of such applications has been issued by the Home Office and will be taken into account when an application is made on behalf of the Council for approval of a RIPA authorisation

PART 7

AUTHORISING OFFICERS

7.1 A RIPA authorisation for Directed Surveillance or CHIS may be issued by any Chief Officer, Assistant Chief Officer, Head of Service, Service Manager or equivalent (The Regulation of Investigatory Powers) Directed Surveillance and Covert Human Intelligence Sources) Order 2010 SI 2010/521) **if they have delegated authority to do so and have received training on the issuing of authorisations.**

7.2 Applications for the acquisition of Communications data can only be issued by a Home Office accredited single point of contact (SPOC). The Council has only one SPOC who is a solicitor in the Legal and Democratic Services Section.

7.3 Detailed advice on the procedures for authorising directed surveillance can be found in the Home Office Revised Code of Practice on Covert Surveillance and Property Interference 2018. Advice on the use of CHIS is contained in the Code of Practice on Covert Human Intelligence Sources 2018. These Codes may be downloaded from the Home Office website.

7.4 It is however important to recognise that only certain sections of RIPA apply to Local Authorities. This part of the policy document wills therefore sumarise the procedure that should be adopted by authorising officers following receipt of an application for a RPIA authorisation.

7.5 **Determining an Application**

The applicant officer must complete the application form in its entirety.

In the case of applications for authority to carry out **directed surveillance** the authorising officer should

Assess whether the investigation falls within the scope of RIPA as amended by the Protection of Freedoms Act 2012.

Consider whether the specific operation or investigation has been adequately described.

Be satisfied as to the reasons for the application n/b **The Council will only use RIPA authorisations relating to directed surveillance for the purpose of preventing or detecting criminal offences carrying a maximum penalty on conviction of at least six months imprisonment.**

Be satisfied that the directed surveillance is necessary

be satisfied that the surveillance is proportionate to the stated purpose and objectives.

Be satisfied that the possibility of collateral surveillance has been avoided or minimised.

Consider the likelihood of confidential information being acquired

Check that an appropriate review period has been listed on the application form.

When presented with an application for authority to conduct or use **CHIS (this can only be used by a local authority for the prevention or detection of crime or the prevention of disorder)** the authorizing officer in addition to being satisfied that the proposed use of CHIS is both necessary and proportionate should also be satisfied that the requirements of section 29 (5) of RIPA and The Regulation of Investigatory Powers (Source Records) Regulations 2000 have been satisfied

In summary this requires the authorising officer to;

Be satisfied that appropriate arrangements are in place for the management and oversight of CHIS and that health and safety issues are addressed through a risk assessment

Consider the likely degree of intrusion of all those affected

Ensure that arrangements are in place to ensure the records contain required particulars and are maintained in such a way as to be unavailable except on a need to know basis.

Consider the likely adverse impact on community confidence that may result from the conduct and use of CHIS

Because the use if CHIS by the Council is likely to be extremely rare advice on the granting of authorisations should normally be sought from the Executive Director Legal and Democratic Services before any are issued.

Applications for an authorisation or notice requiring the provision of communications data will be issued by the Council's Home Office Single Point of Contact Officer who is a solicitor in the Legal and Democratic Services Section.

When considering an application for such an authorisation the authorising officer will:
decide whether a notice or an authorisation is most appropriate
consider whether access to the communications data is reasonably practical for the postal or telecommunications operator
assess the cost and resource implications for both the Council and the postal and telecommunications operator
ensure compliance with any code of conduct issued by the Home Office.

PART 8

WORKING WITH / THROUGH OTHER AGENCIES

8.1 When some other agency has been instructed on behalf of the Council to undertake any action under RIPA this document and the published forms must be used in accordance with the prescribed procedures and the agency advised of the various requirements. The agent must be made aware of exactly what they are authorised to do. It is the responsibility of the officer who instructs the agents to ensure that they comply with RIPA requirements.

8.2 When another agency (e.g. the Police , HMRC etc) wish to use the Council's premises or facilities (other than CCTV) for their own RIPA action officers should normally co-operate unless there are good operational or management reasons as to why the Council's facilities should not be used for the agency's activities. Suitable insurance or other indemnities may be sought from the agency in return for the Council's co-operation. In such cases the Council's RIPA forms should not be used if it is merely assisting and is not actually involved in the RIPA activity.

8.3 Where the Council's premises or facilities (other than CCTV) are being used by some other agency under its own RIPA authorisation then other than in exceptional circumstances where there is a demonstrable need for urgency the other agency should not be permitted to use the Council's premises or facilities until its RIPA has been approved by an authorising officer.

8.4 The operation of the Council's CCTV system has been outsourced to Blackburn with Darwen Borough Council which has agreed to operate the system. The use of the Council's CCTV systems is covered by other policies.

PART 9

RECORD MANAGEMENT

9.1 The Council must keep a detailed record of all authorisations, reviews cancellations renewals and rejections. A central register of RIPA forms will be maintained by the Executive Director Legal and Democratic Services.

9.2 **Records maintained by Service Heads**

The following documents must be retained by the relevant Head of Service (or their designated RIPA co- ordinator)

a copy of the forms relating to the approval, review, cancellation, renewal and rejection of each RIPA authorisation together with any supplementary documentation. Each application should be allocated its own unique reference number “URN”

the date and time when any authorisation was given

a record of the period over which the authorised action has taken place

the frequency of reviews and the outcome of each review.

A copy of each application to the Magistrates Court for approval of a RIPA authorisation.

9.3 Central Register

Applicants must forward a copy of every RIPA application and all forms relating to that application to the Executive Director Legal and Democratic Services within 5 working days of the authorisation, review, renewal, cancellation or rejection of an application.

The Central Register will contain a copy of each application and all other forms relating to it. A record of the details referred to in the appropriate Home Office Code of Practice will also be retained

When an application/ renewal / cancellation form is submitted for inclusion in the Central Register the Executive Director, Legal and Democratic Services or an appointed member of her staff will check the application to monitor compliance with all relevant statutory requirements and the guidance issued from time to time by the Home Office and the Office of Surveillance Commissioners.

The Central Register will be monitored every 6 months and a report to the Council's Cabinet will be submitted by the Executive Director, Legal and Democratic Services every 6 months.

The Executive Director of Legal and Democratic Services shall ensure that records are retained for a period of at least 3 years from the ending of the authorisation. The Office of the Surveillance Commissioners can audit/ review the Council's policies procedures and any individual applications.

9.4 Management of Surveillance Equipment.

The deployment of any equipment used for the purposes of covert surveillance will be managed by Sections Heads in accordance with a protocol prepared the Council's Head of Audit. Each Section Head will maintain a record of the equipment issued by their staff, the investigation in connection with which it is to be used (including any URN) and the identity of the person issued with / using the equipment and the duration of use.

PART 10

TRAINING

10.1 Training on RIPA and the procedures set out in this policy document will be given or authorised by the Executive Director, Legal and Democratic Services. Authorising officers must receive suitable training before signing any RIPA authorisations.

10.7 A central Register of all officers who have received training on RIPA will be maintained by the Executive Director, Legal and Democratic Services.

10.3 As part of the periodic review of this Policy and Authorisation Document the Executive Director Legal and Democratic Services will determine any ongoing training needs both for authorising officers and applicant officers. Refresher course will be held every 2 years or in the event of any significant change in the law or guidance that affects this policy.

10.4 The responsibility for ensuring that staff receive appropriate training in connection with RIPA lies with Chief Officers and Section Heads.

10.5 The purpose of the training will be to ensure that both applicant and authorising officers are not only familiar with the law governing RIPA regulated activities but also receive practical advice on the making and consideration of applications. In particular the training will be aimed at authorising officers with the evidence that is needed to show that a covert operation is necessary, proportionate and likely to be conducted in a manner that will minimize collateral intrusion.

10.6 The training will also emphasise the need for authorising officers to state clearly the nature of the covert activity that they are authorising and the parameters of that activity i.e. what, where, when , how and against whom.

10.7 The importance of setting and observing review cancellations and renewal dates will form part of the training.

ANNEX

Codes of Practice

This policy is not intended to replace or replicate the Guidance issued by the Home Office which is incorporated into this Corporate Policy and Authorisation Procedures and should be referred to in conjunction with it.

Home Office Revised Code of Practice on Covert Surveillance and Property Interference 2018

Home Office Code of Practice on Covert Human Intelligence Sources 2018