Policy Statement
Regulation of Investigatory Powers Act 2000 (RIPA)

November 2016

CONTENTS PAGE

GLOSSARY OF TERMS

1 RIPA – Regulation of Investigatory Powers Act 2000

2 HRA – Human Rights Act 1998

3 CHIS – Covert Human Intelligence Source

4 OSC – Office of Surveillance Commissioners

5 ASB – Anti social behaviour

6 SPOC – Single point of contact

7 URN – Unique Reference Number

8 DVLA – Driver and Vehicle Licensing Agency

1. COMPLAINTS

1.1 South Ribble Borough Council's complaints procedure

If you have any reason to believe that you have been subjected to unauthorised covert surveillance by the Council, or you are unhappy about any other aspect of the Council's operation under RIPA, then you may complain. The Council operates an internal complaints procedure and full details are available on the Council's website www.southribble.gov.uk. Copies are also available on request.

Complaints should be emailed to the Council dwhelan@southribble.gov.uk or sent to the:

Legal Services Manager
South Ribble Borough Council
Civic Centre
West Paddock
Leyland
Lancashire
PR25 1DH

1.2 Independent Tribunal

RIPA establishes an independent tribunal and this tribunal is made up of Senior Members of the Judiciary and the legal profession and is independent of the government. The tribunal has full powers to investigate and decide any case within its jurisdiction.

The Investigatory Powers Tribunal
PO Box 33220
London
SW1H 9ZQ

Tel: 0207 035 3711

Website address: www.ipt-uk.com.

2. Background

The Regulation of Investigatory Powers Act 2000 (RIPA) provides the legislative framework within which covert surveillance operations must be conducted in order to ensure that investigatory powers are used in accordance with human rights. This Policy Statement is intended as a practical reference guide for Council Officers / investigators who may be involved in covert operations.

Officers / investigators involved in covert operations, must familiarise themselves with the Home Office Revised Code of Practice on Covert Surveillance and Property Interference and the Code of Practice on Covert Human Intelligence Sources in order to ensure that they fully understand their responsibilities. The Home Office Codes are available from www.homeoffice.gov.uk/counter-terrorism

Officers/investigators should also familiarise themselves with the Home Office Guidance published in October 2012 – "Protection of Freedoms Act 2012 – changes to provisions under the Regulation of Investigatory Powers Act 2000 (RIPA)"

The Human Rights Act 1998 [HRA] (which brought much of the European Convention on Human Rights and Fundamental Freedom 1950 into UK domestic law) requires the Council, and organisations working on its behalf, pursuant to Article 8 of the European Convention, to respect the private and family life of citizens, their home and their correspondence.

The European convention did not however make this an absolute right, but a qualified right. Accordingly in certain circumstances the Council may interfere in the citizen's right mentioned above, if such interference is: - (a) in accordance with the law; (b) necessary; and (c) proportionate.

RIPA and regulations provide an exemption from the right to privacy in certain circumstances, and allow public bodies to interfere with the individual's right to privacy in circumstances which amount to covert surveillance. However, prior judicial approval must now be obtained for any such operations.

The Council is committed to implementing the provisions of RIPA to ensure that any covert surveillance carried out during the course of investigations is undertaken properly and that the surveillance is necessary and proportionate to the alleged offence/s. The Council seeks to ensure that this Policy Statement remains consistent with the Council's objectives.

This Policy Statement ensures:

- that proper procedures are in place in order to carry out covert surveillance;
- that an individual's right to privacy is not breached without justification;
- that proper authorisation is obtained for covert surveillance;
- that proper procedures are followed;
- that the requisite judicial authority will be sought in all necessary circumstances;
- and that covert surveillance is considered as a last resort having exhausted all other avenues.

If the correct procedures are not followed, evidence may be disallowed by the courts, a complaint of maladministration could be made to the Ombudsman, and/or the Council could be ordered to pay compensation. Such action would not, of course, promote the good reputation of the Council and will, undoubtedly, be the subject of adverse press and media interest. It is essential, therefore, that all involved with RIPA comply with this Document and any further guidance that may be issued, from time to time, by the Council's Legal Services.

Copies of this document can be found on Connect.

---

3. Surveillance

3.1 "Surveillance" includes:-

- monitoring, observing, listening to persons, watching or following their movements, listening to their conversations and other such activities or communications
- recording anything mentioned above in the course of authorised surveillance
- surveillance, by or with, the assistance of appropriate surveillance devices

3.2 What is Overt Surveillance?

Most of the surveillance carried out by the Council will be done overtly – there will be nothing secretive, clandestine or hidden about it. Surveillance will also be overt if the subject has been told it will happen (eg where a noise maker is warned that noise will be recorded if the noise continues). In these circumstances no specific authorisation will be required in RIPA; however, it is always wise to check the situation with Legal Services beforehand.

3.3 What is Covert Surveillance?

(see sections 1.8 – 1.12 of Home Office Covert Surveillance and Property Interference Code of Practice)

Covert surveillance is defined in RIPA as any surveillance which is carried out in a manner calculated to ensure that the persons the subject of the surveillance are unaware that it is or may be taking place. RIPA goes on to define two different 'types' of covert surveillance:

- directed surveillance
- intrusive surveillance

Intrusive surveillance 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 is carried out by means of a surveillance device.

The Council has no powers to undertake intrusive surveillance operations. This form of surveillance can only be carried out by the Police and other law enforcement agencies.

3.4 What is directed surveillance?

(see section 2.2 of Home Office Covert Surveillance and Property Interference Code of Practice)

Directed surveillance is defined in RIPA as surveillance which is covert but not intrusive and is undertaken:

- for the purposes of a specific operation or investigation;

- in such a manner that it is likely to result in the obtaining of private information about a person (whether or not they are the individual specifically identified for the purposes of the operation);

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

3.5 For what purposes can the Council conduct directed surveillance?

(see section 5.1 of Home Office Covert Surveillance and Property Interference Code of Practice)

The Council can use directed surveillance only for the purpose of preventing or detecting crime. Further the offence in question must attract a potential custodial sentence of at least 6 months or involve the sale of alcohol or tobacco to minors.

Notwithstanding any other provisions of this policy where an Officer is contemplating undertaking surveillance that does not fall within the RIPA purpose as detailed above, they must take advice from Legal Services before they proceed.

3.6 What falls within the definition of directed surveillance?

(see various sections including 2.2 to 2.3 and 2.8 of the Home Office Covert Surveillance and Property Interference Code of Practice)

It is safest to assume that any operation that involves planned covert surveillance of a specific person or persons, of however short a duration, falls within the definition of directed surveillance and will, therefore, be subject to authorisation under RIPA. This will also necessitate prior judicial approval.

The consequence of not obtaining an authorisation and the necessary judicial review approval may render the surveillance action unlawful under the HRA, or any evidence obtained may be inadmissible in Court proceedings. It is imperative that Council Officers obtain all necessary approvals/authorisations, where the surveillance is likely to interfere with a person's Article 8 rights to privacy. Obtaining an authorisation will ensure that the surveillance action is carried out in accordance with the law and is subject to stringent safeguards against abuse.

Proper authorisation of surveillance should also ensure the admissibility of evidence under the common law, Police and Criminal Evidence Act 1984 (Section 78) and the HRA.

The Home Office Code on Covert Surveillance makes specific reference to the covert use of overt CCTV systems. The Code clearly indicates that such targeted surveillance activity should be subject to RIPA authorisation.

3.7 Examples not involving Directed Surveillance

Directed surveillance is conducted where it involves the observation of a person or persons with the intention of gathering private information to produce a detailed picture of a person's life, activities and associations. 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 of the European Convention. 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.

Generally speaking the term Private life does not include the general observation which is part of an Enforcement Officer's normal work. For example observing a construction site prior to a visit, videoing scaffold erectors prior to a visit for the purpose of identifying problems, or stopping on a hill and using binoculars to identify where agricultural activities are taking place does not constitute directed surveillance.

3.8 What falls outside of directed surveillance?

(see section 2.21 of the Home Office Covert Surveillance and Property Interference Code of Practice)

Anything which constitutes an immediate response e.g. a Council Officer with regulatory responsibilities may by chance be present when an individual is potentially infringing the law and it is necessary to observe, follow, or engage in other surveillance tactics as an instant response to the situation to gather further information or evidence. Once this immediacy has passed, however, any further covert surveillance of the individual should be subject to RIPA authorisation.

If you have time to think about it, plan it and undertake targeted surveillance on a specific person or persons, you also have the time to consider RIPA requirements and use them when appropriate.

Remember, **IF IN DOUBT GET IT AUTHORISED.**

3.9 What is authorisation?

(see section 3 of the Home Office Covert Surveillance and Property Interference Code of Practice)

Authorisation is the process by which a directed surveillance operation is subject to proper consideration, recording and approval by the Officer conducting the investigation and the Officer authorised to approve it.

An authorisation ensures that all relevant factors have been thoroughly considered and checked. It is also the means by which, in the event of challenge, Council Officers can demonstrate that covert surveillance was lawfully conducted and that is was a fair and reasonable way to proceed, despite the possible intrusion of a person's privacy.

The standard authorisation forms issued by the Home Office and adapted for Council use cover all of the necessary aspects. It is important that these forms are correctly and adequately completed for all directed surveillance operations.

There is one element of the written application that is of particular importance and is an integral part of a number of the questions contained in the standard application form:

Proportionality – this is a fundamental principle embodied in the HRA.

Officers must balance the seriousness of the intrusion into the privacy of the subject of the operation (or any other person who may be affected) against the need for the activity in investigative and operational terms.

The following elements of proportionality should be considered:

- balancing the size and scope of the proposed activity against the gravity and extent of the perceived crime or 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.

- Consideration that the potential criminal offence attracts a custodial sentence of 6 months or more, or involves the sale of alcohol or tobacco to minors

Why officers consider the surveillance to be proportionate in the circumstances must be adequately recorded in the application form. It is not enough to simply have a standard phrase saying that the surveillance is proportionate. The rationale for proceeding with covert surveillance needs to be written and explicit.

Officers must explain in clear terms why the directed surveillance is proportionate to what it seeks to achieve. They must explain how intrusive it might be on the subject of surveillance or on others. Further they must explain why this intrusion is outweighed by the need for surveillance in operational terms. They must address their minds to whether the evidence be obtained by any other means.

Officers should consider the following in framing responses to questions included in the application form:

- What is the nature of the suspected or alleged offence / infringement?

- What, if any, are the alternatives to covert surveillance, i.e. could the information be reasonably obtained by other means?

- If there are other options why have these been rejected in favour of covert surveillance?

- What is the level of intrusion of privacy likely to be? Minimal? Average? Significant? Interference will not be justified if the means used to achieve the aim are excessive in the circumstances of the case. Further, any proposed interference with a person or persons' private, home and family life (HRA Article 8 rights) should be carefully managed and must not be arbitrary or unfair.

- Is it possible that legally privileged, personal confidential information or confidential journalistic material could be acquired?

- Is the privacy of other persons not connected with the investigation likely to be affected? (collateral intrusion).

- What is the desired outcome?

- What is the anticipated benefit to the Council?

Proportionality in this context has nothing whatsoever to do with whether or not the possible benefits of a covert surveillance operation justify the time and money expended by the Council, although Officers will no doubt wish to take this into account.

The Authorising Officer will only grant an authority if covert surveillance is **necessary** in the circumstances of the particular case and only for the purpose of preventing and detecting crime.

The Authorising Officer will give consideration to alternative means of obtaining the information required e.g. by obtaining statements from witnesses (if available).

The Authorising Officer must also pay particular attention to Health and Safety issues that may be raised by any proposed surveillance activity. Under no circumstances, should an Authorising Officer approve any RIPA form unless, and until he is satisfied the health and safety of Council employees/agents are suitably addressed and/or risks minimised, so far as is possible, and proportionate to/with the surveillance being proposed. If the Authorising officer is in any doubt, he should obtain prior guidance on the same from the Chief Executive, and the Council's Health and Safety Officer and/or the Council's Legal Services team.

3.10 Judicial Approval

Once the application has been authorised by the Authorising Officer, the authorisation will require judicial approval by a Magistrate. The Legal Services Manager should be contacted to arrange the court hearing. See the Flow Chart set out in Appendix B to this policy.

3.11 Collateral Intrusion

(see sections 3.8 to 3.11 of the Home Office Covert Surveillance and Property Interference Code of Practice)

An Authorising Officer must take into account – and give proper weight to - the risk of collateral intrusion into the privacy of persons other than those who are the direct subjects of the operational investigation, such as innocent bystanders. Unnecessary intrusion into the lives of those not directly involved in the operation will be avoided wherever possible.

Before granting an authorisation, the Authorising Officer will take into account the possibility that similar surveillance activities are being undertaken by other public authorities.

3.12 Who can authorise surveillance operations?

"Director, Head of Service, Service Manager or equivalent" is the term used for the appropriate level of authorisation within local authorities in the statutory instrument that prescribes the officers, ranks and positions for authorisation purposes (RIPA (Directed Surveillance and Covert Human Intelligence Sources) Order 2010: SI No. 521). Within the Council the following officers will be authorising officers:

- The Director of Development, Enterprise and Communities
- The Head of Shared Assurance Services
- The Chief Executive

Where there is a likelihood that legally privileged, personal confidential information or confidential journalistic material will be acquired as a result of a directed covert surveillance operation, authorisation will be by the Chief Executive. Legal advice must be obtained first before proceeding with any request for such authorisation. The Council will be mindful of whether the provisions of RIPA (Extension of Authorisation Provisions: Legal Consultations) Order 2010 would apply in the particular circumstances of the request.

3.13 What is legally privileged information, personal confidential information or confidential journalistic material?

(see sections 4 of the Home Office Covert Surveillance and Property Interference Code of Practice)

The definitions are detailed in section 4 of the Home Office Covert Surveillance and Property Interference Code of Practice.

If any guidance is required on these issues then please see the Legal Services Team.

3.14 What is the duration of authorisations?

(see sections 5.10 of the Home Office Covert Surveillance and Property Interference Code of Practice and sections 4.17 of the Home Office Covert Human Intelligence Sources (CHIS) Code of Practice)

A written authorisation approved by a Magistrate, for a directed surveillance operation will cease to have effect (unless renewed) at the end of a period of three months beginning with the day on which it took effect e.g. authorised on 20 December 2010: expires 19 March 2011. However, officers should be aware that such directed surveillance must be subject to regular reviews. Except in exceptional circumstances, the review will take place 14 days after a written authorisation has been granted and 24 hours after an urgent authorisation has been granted.

Authorisation for a directed surveillance operation using a human intelligence source (which has also been approved by a Magistrate) will cease to have effect (unless renewed) at the end of a period of 12 months beginning with the day on which it took effect.

3.15 How is an operation reviewed, renewed or cancelled?

(see sections 5.12 – 5.18 of the Home Office Covert Surveillance and Property Interference Code of Practice and sections 4.19 – 4.24 of the Home Office CHIS Code of Practice)

All covert operations or investigations must be effectively assessed and regularly monitored by the Officer conducting the operation and the relevant Authorising Officer. The authorisation process should be viewed as a useful management tool to help Officers to achieve this. Regular reviews of authorisations (for written authorisations reviews should take place every 14 days) should be undertaken to assess the need for surveillance to continue. Responsibility for assessing the appropriate review period rests with the Authorising Officer and this should be as frequently as considered necessary and practicable. There is clear guidance on reviews, renewals and cancellations in the Home Office Codes of Practice and Officers should refer to the appropriate sections for further details.

The standard renewal and cancellation forms issued by the Home Office adapted for Council use cover all the necessary aspects. It is important that these forms are correctly and adequately completed. It is particularly important at the review stage that renewal or cancellation of an operation is considered.

The Authorising Officer who granted or last renewed an authorisation must cancel it, if he is satisfied that the directed surveillance no longer meets the criteria upon which it was originally authorised.

3.16 Criminal prosecution

Once a covert operation results in an individual being under suspicion of having committed a criminal offence, he must be informed of this as promptly as is reasonably practicable if the relevant service group is pursuing the offences internally. In all other cases the police will be informed. This is in order to ensure their right to a fair trial or hearing within a reasonable time in accordance with the Human Rights Act. In a situation where it is considered that a matter gives rise to a potential criminal prosecution, any interview with the suspect must be ‘under caution’ and conducted by a suitably trained officer. If appropriate, the police will be involved immediately to ensure that evidential procedures and the requirements are observed. Authorising Officers will note any recorded material handed over to the police.

4. Covert Human Intelligence Source

4.1 What is a covert human intelligence source (CHIS)?

A person is a CHIS if:

- he establishes or maintains a personal or other relationship with a person for the covert purpose of facilitating the doing of anything falling within the two bullet points below
- he covertly uses such a relationship to obtain information or to provide access to information to another person: or
- he covertly discloses information obtained by the use of such a relationship or as a consequence of the existence of such a relationship.

The Council can use a CHIS only for the purpose of preventing or detecting crime.

4.2 What is likely to fall within the definition of a CHIS for Council purposes?

The use of a CHIS by the Council is likely to be infrequent. This type of source of information will be more commonly used by the Police, Security Service, Customs & Excise, other intelligence services etc. where it is normal practice to use agents, informants and officers working undercover.

The provisions of RIPA are not intended to apply in circumstances where members of the public volunteer information as part of their normal civic duties, or to contact numbers set up to receive information eg Crime stoppers or Anti-fraud Hotline. Members of the public acting in this way would not generally be regarded as sources. However, a member of the public giving information will become a CHIS if the information which he/she covertly passes to the Council has been obtained in the course of (or as a consequence of the existence of) a personal or other relationship. When an informant gives repeat information about a suspect or about a family, and it becomes apparent that the informant may be obtaining that information in the course of a family or neighbourhood relationship, then legal advice must be sought. It is likely that the informant is in reality a CHIS.

The ‘use’ of a source involves 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.

There are occasions, however, when the Council may use a CHIS to obtain information e.g.

- A CHIS may be used as a source to obtain information in respect of an investigation into Housing or Council Tax Benefit Fraud; this may be a Council Officer acting undercover.
- A CHIS may be used as a source to obtain information in respect of an investigation into the loss of monies at Council premises where there are cashier activities; this may be a Council Officer acting undercover.
- A professional witness CHIS posing as a neighbour to obtain evidence.

This list is clearly not definitive. There is an element of judgement involved in determining when an individual taking some part in an investigation may be acting as a CHIS and the matter is not entirely black and white; if in doubt take advice from Legal Services.

Material obtained from a CHIS may be used as evidence in criminal proceedings and the proper authorisation of a CHIS should ensure the legality of such evidence.

4.3 Anti-Social Behaviour (ASB) Activities (e.g. noise, violence, racist, etc)

- Persons who complain about ASB and are asked to keep a diary will not normally be a CHIS and therefore do not require authorisation. However, it is always advisable to take legal advice in this regard.

- Recording the level of the noise (e.g. decibel) will not normally capture private information and, therefore, does not require authorisation.

Recording sound (with a DAT recorder) on private premises could constitute intrusive surveillance, unless it is done overtly. For example, it will be possible to make a recording, if the noisemaker is warned that this will occur if the level of noise continues. Placing a stationary mobile or video camera outside a building to record ASB on residential estates will require prior authorisation.

4.4 Are there any special requirements to observe when using a CHIS?

(various sections including 2.2 of the Home Office Covert Human Intelligence Sources Code of Practice)

Yes.

There are rules about the use of vulnerable adults or juveniles as sources and there are also special requirements with regard to the management, security and welfare of sources. Refer to the procedure on CHIS at Appendix A. The use of a CHIS can only be used if the RIPA procedures are followed.

Where the use of a CHIS is deployed, a 'Handler' (who can be an officer of the Council)) should be designated to have the day to day responsibility for dealing with the CHIS and the security and welfare of the CHIS. Further, a "Controller" should be designated to have the general oversight of the use made of the CHIS. In addition a "Record Keeper" should also be designated. When a CHIS is deployed, records shall be kept to comply with the Home Office Covert Human Intelligence Code of Practice and the Regulation of Investigatory Powers (Source Records) Regulations 2000 (SI 2000/2725).

Tasking is the assignment given to CHIS and can include asking him to obtain information, provide access to information or to otherwise act, incidentally, for the benefit of the relevant public authority. Authorisation for the use or conduct of a CHIS is required prior to any tasking where tasking requires the CHIS to establish or maintain a personal or other relationship for a covert purpose.

4.5 Authorisation/Judicial Approval

Prior to the authorising of a CHIS, the Authorising Officer shall have regard to the safety and welfare of the CHIS and shall continue to have such regard, throughout the use of the CHIS. Where necessary, the safety and welfare of the CHIS should continue to be taken into account after the authorisation has been cancelled or where the investigation has been cancelled or where the investigation has been closed.

An authorisation for a CHIS may be in broad terms and highlight the nature of the CHIS's task. If this changes, then a new authorisation may need to be sought.

Those officers specified in paragraph 3.12 of this Policy will also act as Authorising Officers for the purposes of authorising the use of a CHIS.

As with directed surveillance prior judicial approval will also be sought to the use of a CHIS. Officers should liaise with the Legal Services team to arrange the requisite court hearing.

5.0 Communications Data

5.1 Communications Data Order 2003

The Regulation of Investigatory Powers (Communications Data) Order 2003 extends to local authorities the powers set out within RIPA to access communications data. Communications data includes information relating to the use of a communications service but does not include the contents of the communications itself. Communications data can be split into three types; “traffic data” i.e. where a communication was made from, to whom and when; “service data” is the use made of the service by any person eg itemised telephone records; and “subscriber data” i.e. any other information that is held or obtained by an operator on a person they provide a service to.

Local authorities are allowed to access “service data” and “subscriber data”; they are not allowed to access “traffic data”.

5.2 Authorisation

The order permits access to communications data, by local authorities only where it is necessary for the prevention or detection of crime. As with surveillance, access to communications data should only be authorised where it is proportionate to the objectives the Council is seeking to achieve. It should not be authorised where less intrusive means can be used to further an investigation.

5.3 Alternative methods for authorisation

Access to communications data may be authorised in two ways; either (a) through an authorisation by an Authorising Officer which would allow the authority to collect or retrieve data itself, or (b) by a notice given to a postal or telecommunications operator requiring that operator to collect or retrieve the data and provide it to the local authority.

5.4 Application

Application will be made by the investigating officer and submitted to a Single Point of Contact (SPOC) who will either accept or reject the application. If the SPOC accepts the application he will forward it together with a SPOC report and a draft notice (where appropriate) to an Authorising Officer for authorisation. If the Authorising officer accepts the application, the forms will be returned to the SPOC and the SPOC will deal with the postal or telecommunications operator directly. The SPOC will also advise investigating officers and Authorising officers on whether an authorisation or a notice is appropriate in the circumstances. Authorisations and Notices will now require judicial approval. Authorisations and Notices will be valid for a maximum of one month from the date the Magistrate has approved the grant.

5.5 Training

The officer currently nominated as SPOC is the Legal Services Manager.

The Legal Services Manager will only undertake duties here once he has received training on a course recognised by the Home Office.

5.6 Authorising Officers

Authorising Officers for the purposes of communication data will be the same as for directed surveillance and CHIS's.

6.0 Record Keeping

6.1 How should records be maintained?

(see section 8 of the Home Office Covert Surveillance and Property Interference Code of Practice and sections 2.13 – 2.14, 4.25 – 4.27 of the Home Office CHIS Code of Practice)

The Council must keep a detailed record of all authorisations, renewals, cancellations and rejections in their service areas and a Central register of all Authorisation Forms will be maintained and monitored by the Legal Services Manager. The Legal Services Manager will also keep a detailed record of any judicial approvals granted.

6.2 Records maintained in the service group

The following documents must be retained by the relevant Senior Officer (or his designated Co-ordinator) for such purposes.

- A copy of the forms together with any supplementary documentation and notification of the approval given by the Authorising officer and approval form given by a Magistrate
- 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 given by the Authorising Officer and approval form given by a Magistrate, together with the supporting documentation submitted when the renewal was requested;
- The date and time when any instruction was given by the Authorising Officer;
- The Unique Reference Number for the authorisation (URN).

Each form will have a URN. The service Co-ordinators will issue the relevant URN to Applicants.

The relevant Senior Officer for these purposes will be the Service Manager for the officer who has applied for the authorisation in question. If a Senior Officer is in doubt as to what is required he/she should speak to Legal Services for further guidance.

6.3 Central Register maintained by the Legal Services Manager

Authorising Officers must forward details of each Form to the Legal Services Manager for the Central register, within 1 week of the authorisation, review, renewal, cancellation or rejection.

The Council will retain records for a period of at least three years from the ending of the authorisation. The Office of the Surveillance Commissioners (OSC) can audit/review the Council's policies and procedures, and individual authorisations.

7.0 Role of the Senior Responsible Officer and the RIPA Monitoring Officer

7.1 Who is the Senior Responsible Officer?

The Director of Governance and Business Transformation is the Council's Senior Responsible Officer.

7.2 Duties of the Senior Responsible Officer

The Senior Responsible Officer will be responsible for the following:

- The integrity of the processes in place within this Council dealing with the authorising of directed surveillance, the use of covert human intelligence sources and the accessing of communications data
- Compliance with all relevant statutory provisions and associated guidance
- Engagement with the Commissioners and Inspectors when they conduct their inspections
- Where necessary, overseeing the implementation of any post-inspection action plans recommended or approved by a Commissioner
- Ensuring that all authorising officers are of an appropriate standard in the light of any recommendations in the inspection reports prepared by the Office of the Surveillance Commissioner

7.3 Who is the RIPA Administrative Officer?

The Legal Services Manager is the Council's RIPA Administrative Officer

7.4 Duties of the RIPA Administrative Officer

The RIPA Administrative Officer will be responsible for the following:

- Maintaining the Central Record of authorisations and collating the original applications/authorisations, reviews, renewals and cancellations
- Oversight of submitted RIPA documentation
- Organising and maintaining a RIPA training programme
- Raising RIPA awareness within the Council

7.5 Role of Governance Committee

Twice yearly the Senior Responsible Officer shall report to the Council's Governance Committee on the Council's use of its RIPA powers. Governance Committee should also review the Council's Policy document at least once every two years or sooner if a change of legislation requires it. More regular reports will be taken to Governance Committee on the use of RIPA powers if either the Governance Committee or the Senior Responsible Officer considers this to be desirable. In no circumstances will Governance Committee – or any elected member for that matter – make a

decision on any specific authorisations – such decisions can only be made by the Authorising Officers specified in paragraph 3.12 of this policy.

8.0 Covert Surveillance of Social Networking Sites

In certain circumstances, use of social media sites such as Facebook, or using the internet for research in other ways could need authorisation as directed surveillance or use of a covert human intelligence source. The Office of Surveillance Commissioners has given guidance on when the use of social media and the internet might need authorisation on RIPA. You can read the guidance at Appendix C.

APPENDIX A

AUTHORISATION PROCEDURE

DIRECTED SURVEILLANCE

1. Must be authorised in accordance with paragraph 3.12 of this policy.

2. The Authorising Officer must firstly, satisfy themselves that the authorisation is necessary for the purpose of preventing and detecting crime. This is the only ground the Council can rely on.

3. The Authorising Officer should then satisfy themselves that the surveillance is proportionate to what it seeks to achieve. In many instances, evidence may be obtainable by other routes, other than directed surveillance, e.g. witness statements, official records, the DVLA, etc.

4. The Authorising Officer has to be satisfied that the specific targeted criminal offence carries a maximum custodial sentence of 6 months or more.

5. As part of that judgement, the Authorising Officer should consider whether there could be any collateral intrusion on, or interference with, the privacy of person(s), other than the subject of the surveillance. This is particularly relevant where the premises being observed is used by other persons. This must be taken into account by the Authorising Officer when considering whether the need for the surveillance is proportionate to the problem.

6. As a matter of policy, no directed surveillance should be carried out by Council staff which may intrude upon circumstances covered by the Seal of the Confession, which refers to the spiritual counselling between a Minister and a Member of their faith.

7. A form has been devised for use when authorisation for directed surveillance is being sought, and granted. The form should be completed by the Officer wishing to carry out the directed surveillance and the Authorising Officer, together with approval from a Magistrate, before any directed surveillance takes place. Copies of this form (and all other forms relating to the use of directed surveillance) may be obtained from the Legal Services Manager.

8. In urgent cases only, authorisation may be given orally, however, please note that judicial approval will be required, prior to any directed surveillance. The form must be completed as soon as possible. In such cases, the Authorising Officer will also need to make a written statement to show that they have expressly authorised the surveillance, and why it was necessary to give oral approval in the first instance.

9. Directed surveillance might be employed by other agencies with which the Council carries out joint investigations, for example the Police or the Environment Agency. In those instances,

care should be taken to determine whether there will be directed surveillance, who by, and who will be authorising its use. It is normally for the tasking agency to obtain or provide the authorisation. If the Council decides that directed surveillance is necessary, then it should inform those in the other agencies involved in the joint investigation.

10. The authorisation for directed surveillance, and any associated papers should be retained on the Service file for a period of at least 3 years. A copy of the authorisation must be forwarded to the Legal Services Manager who will arrange for the information to be held centrally and recorded on a register.

11. The Legal Services Manager will on request, make the authorisations available for inspection, by the Office of Surveillance Commissioners (OSC) and to the investigatory Powers Tribunal.

12. Any material produced as a result of directed surveillance must be retained for only as long as it is necessary. It should be disposed of in accordance with the Criminal Procedures and Investigations Act 1996.

13. Authorising Officers must ensure compliance with the Data Protection Act 1998 principles.

CONFIDENTIAL MATERIAL

'Confidential material' is described by RIPA as being:

a. matters subject to legal privilege;

b. confidential personal information; or

c. confidential journalistic material.

Where there is a likelihood that confidential material will be acquired as a result of a directed covert surveillance operation, authorisation will be by the Chief Executive. Legal advice shall be obtained first before proceeding with any request for such authorisation.

Acquiring confidential material concerning the object of the surveillance is likely to be rare. Confidential material is more likely to come into the possession of those carrying out other types of intrusive surveillance by means of surveillance devices, such as bugs placed in vehicles and residential premises.

COVERT HUMAN INTELLIGENCE SOURCE (CHIS)

1. Must be authorised by an Officer specified in paragraph 3.12 of this policy as 'Authorising Officer.'

2. The Authorising Officer must firstly, satisfy themselves that the authorisation is necessary for the purpose of preventing or detecting crime. This is the only ground the Council can rely on.

3 The Authorising Officer should satisfy themselves that the use of CHIS is proportionate to what it seeks to achieve and that it is necessary. In many instances, evidence may be obtainable by other routes, other than the use of a CHIS, e.g. witness statements.

4. As part of that judgement, the Authorising Officer should consider whether there could be any collateral intrusion on, or interference with, the privacy of person(s), other than the subject of the covert surveillance.

5. A form has been devised for use when authorisation for a CHIS is being sought, and granted. The form should be completed by the Officer wishing to carry out covert surveillance and the Authorising Officer should approve, together with judicial approval by a Magistrate before any surveillance takes place. A copy of this form (and all other forms relevant to the authorisation of a CHIS) may be obtained from the Legal Services Manager.

6. CHIS might be employed by other agencies with which the Council carries out joint investigations, for example the Police or the Environment Agency. In those instances, care should be taken to determine whether there will be covert surveillance, who by, and who will be authorising its use. It is normally for the tasking agency to obtain or provide the authorisation. If the Council decides that a CHIS is necessary, then it should inform those in the other agencies involved in the Joint investigation.

7. The Authorising Officer must be satisfied that the appropriate arrangements are in place for the management of the CHIS. This should include a risk assessment for health and safety.

8. The Authorising Officer should consider the diverse impact on community confidence that may result from the information obtained.

9. The authorisation for a CHIS, and any associated papers should be retained on the Departmental file for a period of at least 3 years. A copy of the authorisation must be forwarded to the Legal Services Manager who will arrange for the information to be held centrally and recorded on a register.

10. The Legal Services Manager will on request, make the authorisations available for inspection, by the Office of Surveillance Commissioners (OSC) and to the investigatory Powers Tribunal.

11. Any material produced as a result of a CHIS must be retained for only as long as it is necessary.

12. Authorising Officers must ensure compliance with the Date Protection Act 1998 principles.

REVIEW

Regular reviews will take place once authorisation has been granted. Except in exceptional circumstances, the review will take place 14 days after a written authorisation has been granted and 24 hours after an urgent authorisation has been granted. Records of reviews will be maintained in the Departmental file and centrally, by the Legal Services Manager. Records will be retained in both locations for a period of 3 years.

All necessary forms relating to reviews may be obtained via the Legal Services Manager.

RENEWALS

It will be rare that renewals of authorisations will be required in order to continue surveillance. However, if they are required, applications for renewals of authorisation will be made in writing using a standard renewal proforma.

All necessary forms relating to renewals may be obtained via the Legal Services Manager.

If the Authorising Officer considers it necessary for the authorisation to continue, then it may be renewed as follows:

- For an ordinary authorisation, renewed for a period of up to three months.

- For an urgent oral authorisation, renewed for a period of up to 72 hours.

Please note that renewals will also require judicial approval by a Magistrate and therefore a further application to court will be necessary.

All applications for renewals will contain the following information:

- Renewal numbers and dates of any previous renewals;
- Details of any significant changes to the information as listed in the original authorisation as it applies at the time of the renewal;
- Details of the reasons why it is necessary to continue with the directed surveillance;
- Details as to why the directed surveillance is still proportionate to what it seeks to achieve;
- An Indication of the content and value to the investigation or operation of the information so far obtained by the directed surveillance;
- Details of the results of the regular reviews of the investigation or operation.

Records of renewals will be maintained in the service group file and centrally, by the Legal Services Manager. Records will be retained in both locations for a period of 3 years.

CANCELLATION

1. Authority to carry out covert surveillance is valid for a period of 3 months, from the date it was granted. However, there is a duty incumbent upon both the Authorising Officer and the Officer carrying out the surveillance, to continually review its necessity and proportionality. The operation must be cancelled as soon as it is no longer appropriate, irrespective of the time outstanding. The cancellation must be recorded in writing on the appropriate authorisation form and retained in the service group file and centrally, by the Legal Services Manager.

2. As soon as the decision is made to cancel the authorisation, an instruction will be given to those carrying out the investigation to stop all surveillance.

3. Due to the nature of the Council's likely use of directed surveillance, permission to renew / extend directed surveillance will only be granted on an exceptional basis. The request for renewal / extension must be accompanied by detailed information about the investigation, and reasons why directed surveillance must be continued. The application and any authorisation of a renewal / extension must be retained on the service group file and copied to the Legal Services Manager. Records will be retained in both locations for a period of 3 years. No form is provided for renewing / extending approvals. The circumstances will be so unique, that it must be argued on a case by case basis.

MATERIAL OBTAINED

Material obtained as a result of an investigation involving covert surveillance will be afforded special protection in relation to handling and storage.

Confidential material will not be retained or copied unless it is necessary for a specific purpose.

All material obtained as a result of having undertaken a directed covert surveillance will be recorded and logged in the investigating officer's notebook in accordance with usual procedures for logging of evidence.

Confidential material will only be disseminated outside the Council where this has been expressly authorised by the Authorising Officer, having taken the necessary legal advice.

Reasonable steps will be taken to ensure that confidential information is securely stored and cannot fall into the wrong hands.

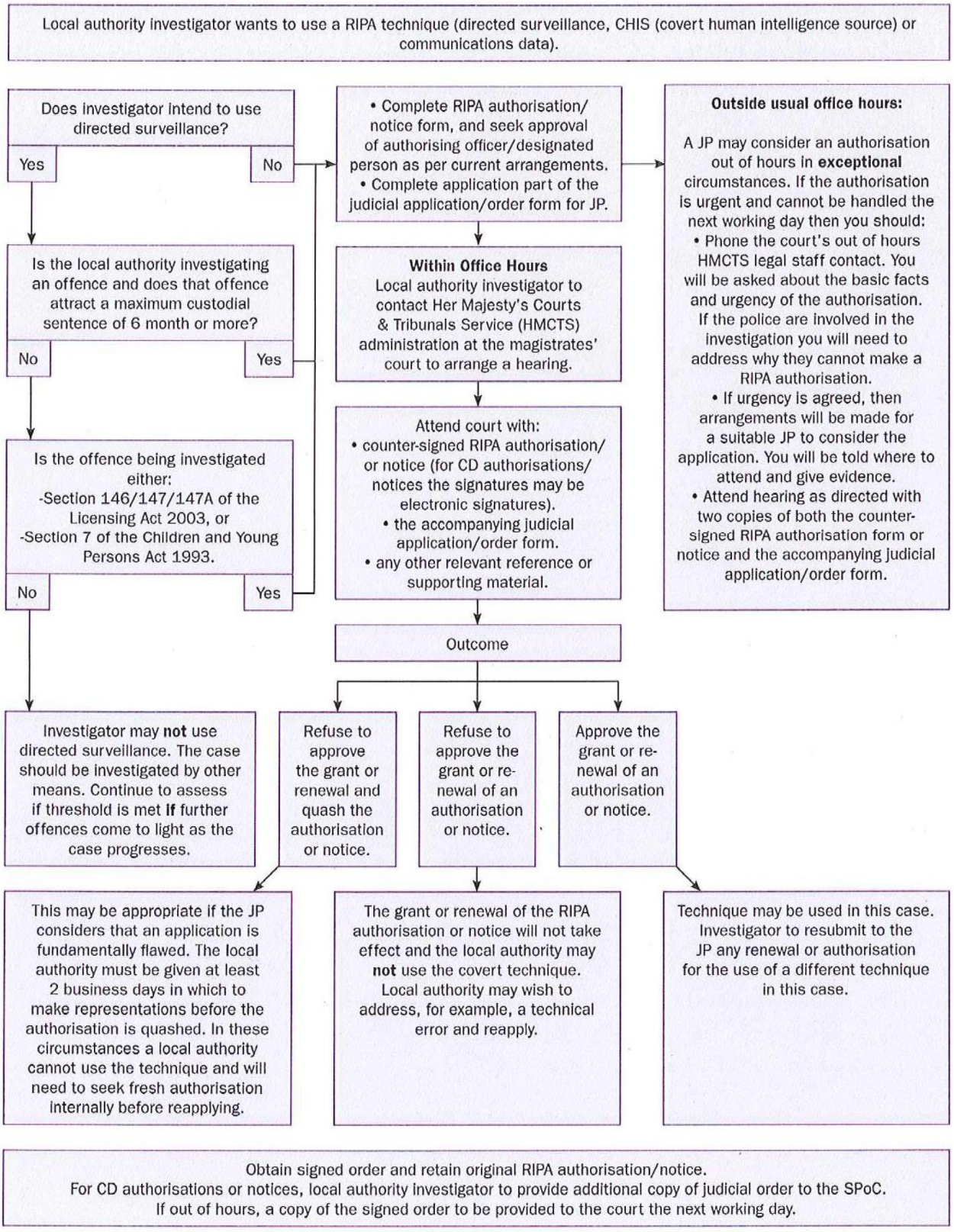
All confidential information will be destroyed as soon as it is no longer necessary to retain it for the specified purpose. Regular review of material obtained as a result of covert surveillance will ensure that material is destroyed when its retention can no longer be justified.

TRAINING

All investigators and Authorising Officers are adequately trained on the provisions of RIPA to ensure that the requirements of the law are complied with. Regular up date training is provided, to ensure that all personnel involved with the operation of the law are aware of its requirements.

APPENDIX B

LOCAL AUTHORITY PROCEDURE: APPLICATION TO A JUSTICE OF THE PEACE SEEKING AN ORDER TO APPROVE THE GRANT OF A RIPA AUTHORISATION OR NOTICE



APPENDIX C

Guidance on Covert Surveillance of Social Networking Sites

The Office of Surveillance Commissioners

The fact that digital investigation is routine or easy to conduct does not reduce the need for authorisation. Care must be taken to understand how the SNS being used works. Authorising Officers must not be tempted to assume that one service provider is the same as another or that the services provided by a single provider are the same.

Whilst it is the responsibility of an individual to set privacy settings to protect unsolicited access to private information, and even though data may be deemed published and no longer under the control of the author, it is unwise to regard it as “open source” or publicly available; the author has a reasonable expectation of privacy if access controls are applied. In some cases data may be deemed private communication still in transmission (instant messages for example). Where privacy settings are available but not applied the data may be considered open source and an authorisation is not usually required. Repeat viewing of “open source” sites may constitute directed surveillance on a case by case basis and this should be borne in mind.

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

It is not unlawful for a member of a public authority to set up a false identity but it is inadvisable for a member of a public authority to do so for a covert purpose without an authorisation for directed surveillance when private information is likely to be obtained. The SRO should be satisfied that there is a process in place to ensure compliance with the legislation. Using photographs of other persons without their permission to support the false identity infringes other laws.

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

SOUTH RIBBLE BOROUGH COUNCIL’S POLICY STATEMENT:

The Borough Council takes seriously its statutory responsibilities and will, at all times, act in accordance with the law and take necessary and proportionate action in these types of matters. In that regard, the Council’s Legal Services Manager, is duly authorised by the Council to keep this Document up to date and to amend, delete, add or substitute relevant provisions, as necessary. For administration and operational effectiveness, the Legal Services Manager is also authorised to add or substitute officers authorised for the purpose of RIPA.

.