APPENDIX A

NORTH HERTFORDSHIRE DISTRICT COUNCIL

REGULATION OF INVESTIGATORY POWERS ACT 2000 (RIPA)

POLICY & PROCEDURES

REGULATION OF INVESTIGATORY POWERS ACT 2000

POLICY AND PROCEDURES

CONTENTS

1 INTRODUCTION & BACKGROUND

1.1 This Policy is the framework on which the Council applies the provisions of The Regulation of Investigatory Powers Act 2000 (RIPA) as it relates to covert surveillance. It must be read in conjunction with the statutory codes of practice issued by the Secretary of State and any additional guidance provided by Investigatory Powers Commissioner's Office (IPCO) (formerly the Office of Surveillance Commissioners – OSC) and individual Directorates to deal with the specific issues of their service.

1.2 For the avoidance of doubt, all references to the Home Office Codes of Practice relate to the latest versions which were issued in August 2018 in relation to covert surveillance and covert human intelligence sources; and 2016 in relation to the acquisition and disclosure of communications data. References to the OSC Procedures and Guidance document relate to the latest version which was issued in July 2016

1.3 The Human Rights Act 2000 requires the Council to have respect for the private and family life of citizens. However in rare cases, it may be lawful, necessary and proportionate for the Council to act covertly in ways that may interfere with an individual's rights.

1.4 The rights conferred by Article 8 of the Human Rights Act are qualified so it is still possible for a public authority to infringe those rights providing the following criteria are satisfied;

1.4.1 **It is done in accordance with the law**

1.4.2 **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.

1.4.3 **It is proportionate:** Judging proportionality will probably involve three considerations.

- Is the proposed method of surveillance excessive in relation to the seriousness of the matter that is being investigated? Is it proportional to the mischief under investigation?

- Is there a reasonable available alternative method of investigation that would be less intrusive of privacy rights? i.e. It is the only option, other overt means having been considered and discounted.

- Can collateral intrusion be avoided, and is the surveillance proportional to the degree of anticipated intrusion on the target and others? In addition to the subject there may be a possibility that the privacy rights of a third party may be infringed during surveillance.

1.5 It is possible that unauthorised surveillance will be a breach of a person's right to privacy under Article 8. Even if surveillance without due authorisation

in a particular instance is not illegal, if authorisation is not obtained, the surveillance carried out will not have the protection that RIPA affords.

1.6 If the correct procedures are not followed:

- The authorisation will not take effect as it will not be approved by the Magistrates Court if there are not reasonable grounds
- Court proceedings that rely upon the information obtained by surveillance may be undermined
- A complaint of maladministration may be made to the Ombudsman
- The Council could be the subject of an adverse report by the Investigatory Powers Commissioner's Office
- A claim could be made leading to the payment of compensation by the Council

1.7 Through the application of authorisation procedures and Magistrates Court approval RIPA ensures that a balance is maintained between the public interest and the human rights of individuals.

1.8 RIPA does not;

- Make unlawful anything that is otherwise lawful

- Impose any new statutory duties (N.B. but see paragraphs 1.5 –1.7 on the possible consequences of non compliance)

- Prejudice or disapply 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).

1.9 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.

1.10 It is important to note that the legislation does not only affect directly employed Council staff. Where external agencies are working for North Hertfordshire District Council, carrying out the Authority's statutory functions, the Authority remains liable for compliance with its duties. It is essential that all external agencies comply with the regulations, as they are contractually obliged to do so. Therefore, work carried out by agencies on the Council's behalf should be properly authorised by one of the Council's designated Authorising Officers and requires Magistrates Court approval. Authorisation for surveillance should not be sought on behalf of another statutory or other organisation or agency. The advice of the Monitoring Officer should be sought in the event of uncertainty.

1.11 Applications to the Magistrates' Court for approval of an authorisation must be made in accordance with the requirements of the Court.

1.12 The use of the powers conferred by RIPA is subject to scrutiny by the Investigatory Powers Commissioner's Office, which carries out periodic

inspections of the Council's practices and procedures. Furthermore RIPA also provides for the establishment of a Tribunal to determine complaints about the use of RIPA powers. It is therefore essential that surveillance is always carried out in compliance with RIPA, the policies and codes of practice referred to in this document and any advice or guidance that may be issued from time to time by the Service Director: Legal and Community.

1.13 RIPA provides a means of authorising certain acts of covert surveillance for a variety of purposes. To fully understand the effects of RIPA, it is essential to understand the various types of activity that are covered, and those that are not permitted, and the purposes that will justify surveillance.

1.14 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 (Part 4)**
- **The Acquisition and Disclosure of Communications Data (Part 5)**

2. SURVEILLANCE

2.1 Local Authorities and the Police are permitted under RIPA to carry out covert directed surveillance and to use covert human intelligence sources the definitions for each being as follows;

2.2 **"Surveillance"** includes:

- Monitoring, observing, listening to persons, watching or following 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, which will include cameras, video, and listening or recording devices.

Surveillance can be either **overt** or **covert**.

2.3 Overt Surveillance

2.3.1 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.

2.3.2 Surveillance will be overt if the subject has been told it will happen. This will be the case where a noisemaker is warned that recordings will be made if the noise continues; or where an entertainment licence is issued subject to conditions, and the licensee is told that officers may visit without notice or without identifying themselves to the owner/proprietor to check that the conditions are being met. Such warnings should be given to the person concerned in writing.

2.3.3 Overt surveillance does not require any authorisation under RIPA. Neither does low-level surveillance consisting of general observations in the course of law enforcement (for example, an officer visiting a site to check whether a criminal offence had been committed). Repeated visits may amount to systematic surveillance however, and require authorisation: if in doubt, advice should be sought from the RIPA Monitoring Officer or the Senior Responsible Officer

2.3.4 Home Office guidance also suggests that the use of equipment such as binoculars or cameras, to reinforce normal sensory perception by enforcement officers as part of general observation does not need to be regulated by RIPA, as long as the systematic surveillance of an individual is not involved. However, if binoculars or cameras are used in relation to anything taking place on any residential premises, or in any private vehicle, the surveillance can be intrusive even if the use is only fleeting. Any such surveillance will be intrusive "if it consistently provides information of the same quality as might be expected to be obtained from a device actually present on the premises or in the vehicle". The quality of the image obtained rather than the duration of the observation is what is determinative. It should be remembered that the council is not permitted to undertake intrusive surveillance.

2.3.5 Use of body worn cameras should be overt. Badges should be worn by officers stating body cameras are in use and it should be announced that recording is taking place. In addition, cameras should only be switched on when recording is necessary – for example, when issuing parking tickets.

2.4 Covert Surveillance

Covert surveillance is covert where it is 'carried out in a manner **calculated** to ensure that the person or persons subject to the surveillance are unaware that it is or may be taking place'.

RIPA requires the authorisation of two types of covert surveillance (directed surveillance and intrusive surveillance) plus the use of covert human intelligence sources (CHIS) or acquisition of communications data.

2.5 Covert Human Intelligence Source (CHIS)

2.5.1 A person is a covert human intelligence source if 'he establishes or maintains a personal or other relationship with a person for the covert purpose of obtaining information or providing access to any information to another person, or he covertly discloses information obtained by the use of such a relationship'. Covert in this context means that it is calculated that the subject should be unaware of the purpose of the relationship.

A member of the public who volunteers information to the Council is not a covert human intelligence source.

2.5.2 The conduct or use of CHIS must be authorised in accordance with RIPA.

Conduct of a 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.

The use of a juvenile CHIS may only be authorised for one month at a time.

2.5.3 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.

2.5.4 Noise

Persons who complain about excessive noise, and are asked to keep a noise diary, will not normally be a CHIS, as they are not required to establish or maintain a relationship for a covert purpose. Recording the level of noise (e.g. the decibel level) will not normally capture private information, and therefore does not require authorisation. Recording sound with a DAT recorder or similar, could constitute intrusive surveillance, unless it is done overtly – for example it will be possible to record sound if the noisemaker is warned that this will occur if the level of noise continues.

However, if the Council serves notice on the owner/occupier of the premises and the source of the noise is a third party, authorisation under RIPA may be required. The investigation may (i) be covert in relation to that third party and (ii) may reveal private information about them.

2.5.5 Test Purchases

Carrying out test purchases will not normally require the purchaser to establish a relationship with the supplier with the covert purpose of obtaining information, and therefore the purchaser will not normally be a CHIS. For example, authorisation would not normally be required for test purchases carried out in the ordinary course of business (e.g. walking into a shop and purchasing a product over the counter). By contrast, developing a relationship with a person in the shop, to obtain information about the seller's suppliers of an illegal product e.g. illegally imported wild meat, is likely to require authorisation as a CHIS. Similarly, using hidden recording devices to record what is going on in the shop (e.g. a hidden CCTV Camera) may require authorisation as directed surveillance. A combined authorisation can be provided if a CHIS is carrying out directed surveillance.

2.5.6 **Note 251 of the OSC's 2016 Procedures & Guidance document states:**
251. A local authority may prefer to seek the assistance of the police or another public authority to manage its CHIS. In such a case a written protocol between the parties should be produced in order to ensure that an identified CHIS is properly managed (see CHIS Code of Practice 6.12). In the absence

of such an agreement the local authority must be capable of fulfilling its statutory responsibilities.

2.6 Directed surveillance

Directed Surveillance is surveillance that is:

- covert but not intrusive surveillance; (see paragraph 3.2)
- 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).

2.7 Surveillance by way of an immediate response to events or circumstances where it would not be 'reasonably practicable' for an authorisation to be sought is not included within the provisions of RIPA.

2.8 **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.

3 EXCLUSIONS

3.1 There are some instances where surveillance is not permissible in any circumstances:

3.2 Intrusive Surveillance

RIPA provides that the Council **cannot** authorise intrusive surveillance. This is covert surveillance carried out in relation to anything taking place on residential premises or in any private vehicle, whether by way of a person or device.

It will also be intrusive surveillance where a device placed outside consistently provides information of the same or equivalent quality and detail, as might be expected if it were in the premises or vehicle

Residential premises are any part of premises occupied for residential purposes or living accommodation, including hotel rooms or prison cells. However, it does not include common areas in blocks of flats and similar premises.

Private vehicle is a vehicle used primarily for private purposes by the owner or person entitled to use it.

Only the police or other law enforcement agencies are permitted to employ intrusive surveillance. Likewise, the council has no statutory powers to interfere with private property.

3.3 Use of Children to gather information about parent/ guardian

Authorisation may not be granted for the conduct or use of a source under the age of sixteen where it is intended that the purpose is to obtain information about his parent or any person who has parental responsibility for him.

3.4 Vulnerable Individuals

A vulnerable individual is a person who is, or may be, in need of community care services by reason of mental or other disability, age or illness and who is or may be unable to take care of 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.

4 GROUNDS FOR SURVEILLANCE

4.1 Amendments to the Regulation of Investigatory Powers (Directed Surveillance and Covert Human Intelligence Sources) Order 2010 (“the 2010 Order”) mean that a local authority can now only grant an authorisation under RIPA for the use of Directed Surveillance where the local authority is investigating criminal offences which attract a custodial sentence of a maximum term of at least 6 months' imprisonment, or criminal offences relating to the underage sale of alcohol or tobacco under sections 146, 147 or 147A of the Licensing Act 2003 or section 7 of the Children and Young Persons Act 1933.

4.2 Even if the person granting the authorisation believes that the authorisation is necessary, he must also be satisfied that the authorised activity is proportionate to what is sought to be achieved by it. This requires the Authorising Officer to balance the need for surveillance with the level of intrusion into any person’s privacy.

4.3 Particular consideration should be given to collateral intrusion, which is interference with the privacy of persons other than the subject(s) of the surveillance. Such collateral intrusion or interference would be a matter of

greater concern in cases where there are special sensitivities, for example in cases of premises used by lawyers or for any form of medical or professional counselling or therapy.

4.4 Confidential information

Careful consideration is also needed when there is a risk of obtaining confidential information. This consists of matters subject to

- legal privilege, which is communication between a lawyer and client;
- confidential personal information relating to physical or mental health; or to spiritual counselling or other assistance given or to be given, and which a person has acquired or created in the course of any trade, business, profession or other occupation, or for the purposes of any paid or unpaid office where there is an undertaking to hold it in confidence; or
- confidential journalistic material.

In cases where it is likely that confidential information will be acquired the authorisation must be granted by the Chief Executive as Head of the Paid Service (or in his absence by an authorised Chief Officer)

4.5 An application for an authorisation must include a full assessment of the risk of any collateral intrusion or interference so that the Authorising Officer can consider this.

4.6 Authorising Officers must always consider the need for surveillance or CHIS and balance this against an individual's right to privacy under the Human Rights Act 1998. An officer seeking an authorisation should always be able to justify why it is necessary and why other, less intrusive, forms of investigation are unsuitable or have previously been tried without success and thus the matter has escalated to the requirement for covert surveillance.

5 ACQUISITION AND DISCLOSURE 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.**

5.2 The Information can be obtained in two ways:

- by Authorisation
- by Notice.

5.3 An authorisation, with Magistrates Court approval, 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.

5.4 **An authorisation or notice can only be obtained where it is necessary for the purpose of preventing or detecting crime or of preventing disorder.**

5.5 **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 part 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).**

5.6 **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 following Magistrates' Court approval **and should be renewed or cancelled as appropriate.**

6. PROCEDURE TO OBTAIN 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 and Magistrates Court approval.

6.2 The Council will only very occasionally make use of CHIS so the applicant officer should consult the Monitoring Officer 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 Monitoring Officer before making an application in order to ensure that current statutory requirements and best practice are being observed.

6.4 All applications for authorisation must be sought and granted *before* any surveillance activity takes place. The decision whether or not to authorise an application must not be taken with the benefit of hindsight. This should be borne in mind when submitting an application to the Magistrates' Court under Paragraph 7 below.

6.5 Making the Application

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

- read this policy document
- determine whether the activity that they are proposing to conduct involves directed surveillance or the use of a CHIS
- assess whether the activity will be in accordance with the law – is it 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.

6.6 The application form once completed by the applicant officer, must be submitted to an Authorising Officer, together with a health and safety risk assessment that should cover any potential risks to Council officers, or third parties, including members of the public.

6.7 The persons entitled to grant authorisations are designated in the Schedule of Authorising Officers, which is kept by the Monitoring Officer and is accessible on the Council's Intranet

6.8 The Authorising Officer should note:

- the date and time of grant or refusal;
- the reasons for that decision;
- the exact date on which the authorisation will be reviewed.

6.9 An application must describe:

- any conduct to be authorised;
- the purpose of the investigation and how long the situation has existed;
- why it is necessary;
- why it is proportionate;
- the intended subjects, if known;
- the intended product that the surveillance will provide;
- any potential collateral intrusion and the justification for this;
- details of any confidential information that may be obtained;

6.10 The Application Forms

6.10.1 The Home Office has published standard forms for the use by local authorities. These have been adopted by the Council and can be accessed through the Intranet under *Corporate – Forms - RIPA*. Every box in the application form must be completed or marked n/a where it is not appropriate.

6.10.2 Each operation/ investigation must be allocated a unique reference number (URN). This will be the next number in sequence taken from the Central RIPA Log, as identified by the Authorising Officer and should be entered on the form.

7. MAGISTRATES' COURT APPROVAL

7.1 All RIPA authorisations will require Magistrates' Court approval in the form of an order to take effect. The court must be satisfied that reasonable grounds exist in relation to the authorisation.

7.2 Legal Services must be consulted on the form and content of the application to the Magistrates' Court for approval.

8 DURATION OF AUTHORISATIONS

8.1 It is no longer possible for urgent authorisations to be given orally. However, a Magistrate may consider an authorisation out of hours in exceptional circumstances.

8.2 Directed surveillance authorisations 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:

- three months' is deemed for the purpose of this guidance to mean three calendar months/twelve weeks from the start date of the operations

8.3 Authorisations for the conduct or the use of covert human intelligence sources will last for up to 12 months, beginning with the day on which the grant or renewal takes effect.

8.4 Authorisations relating to communications data last 1 month.

8.5 **Review**

8.5.1 The Authorising Officer must review authorisations frequently, at least monthly. The frequency of mid term reviews should be risk assessed based on the nature of the operation.

8.5.2 RIPA application forms must be reviewed on or before the expiry date of the authorisation which will be the date stated in the application form. When a RIPA authorisation is reviewed the appropriate form should be completed and record:

- the date and time of that review
- confirmation as to whether the surveillance is to continue or not
- the reasons for that decision

8.6 **Renewal**

8.6.1 If at any time before an authorisation would cease to have effect, it is necessary for the authorisation to continue for the purpose for which it was given, it may be renewed in writing for a further period of 3 calendar months, beginning with the day when the original authorisation would have expired. Magistrates Court approval is required before a renewal takes effect.

8.6.2 The Authorising Officer must consider the matter afresh, including taking into account the benefits of the surveillance to date and any collateral intrusion that has occurred.

8.6.3 Authorisations may be renewed more than once, provided they continue to meet the criteria for authorisation and are approved by the Magistrates' Court.

8.6.4 Prior to renewal of an authorisation for the use or conduct of a covert human intelligence source, there must be a full review of the use made of that source, the tasks given to that source and the information so obtained.

8.7 **Cancellation**

8.7.1 The Authorising Officer must cancel an authorisation if they become satisfied that the surveillance is no longer required or appropriate.

8.7.2 Authorisations should not be allowed simply to lapse. The matter should be referred to an Authorising Officer via the same process as for the initial application and a form of cancellation must be completed:

- if the necessary evidence has been obtained; or
- it is decided at any time that the surveillance is unlikely to produce the evidence sought, then.

8.7.3 The Authorising Officer must then cancel the Application without delay. When cancelling the authorisation the Authorising Officer is required to consider whether the surveillance was effective, necessary and met its objectives. Cancellations must be made using the cancellation form and should briefly detail what product(s) resulted from the surveillance.

8.7.4 When cancelling an authorisation, the Authorising Officer must ascertain what recorded material has been obtained by the use of directed surveillance. The

Authorising Officer should comment on the recorded material and how it is to be managed or used thereafter. If the matter is not proceeding to a prosecution, the Authorising Officer must be satisfied that any recorded material has been securely destroyed.

9 AUTHORISING OFFICERS

9.1 Authorisations may only be given by the Authorising Officers listed in Appendix B. Only the Chief Executive can authorise the use of a CHIS, or the acquisition of confidential information.

9.2 Applications for the acquisition of Communications data can only be issued by a Home Office accredited single point of contact (SPoC). The Council has two SPOos, Service Director: Customers and the Investigations Manager.

9.3 The National Anti-Fraud Network (NAFN) provides a SPoC service to local authorities. Local authorities using the NAFN SPoC service will still be responsible for submitting any applications to a Magistrate and a designated person in the authority is still required to scrutinise and approve any applications.

9.4 **Determining an Application**

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

Authorisation under RIPA is quite separate from delegated authority to act under the Council's Scheme of Delegation. **RIPA authorisations are for specific investigations only and must be cancelled or renewed once the specific surveillance is complete, or about to expire.**

The Authorising Officer should not just "sign off" an authorisation, but must give **personal consideration** to the necessity and proportionality of the proposed action prior to applying to the Magistrates Court for approval and must personally ensure that the surveillance is reviewed and cancelled.

Any rejected applications must be entered into the RIPA log held by the Service Director: Legal and Community.

9.5 In the case of applications for authority to carry out **directed surveillance** the Authorising Officer should:

- consider the relevant Codes of Practice
- consider whether the specific operation or investigation has been adequately described
- be satisfied as to the reasons for the application. **N.B. A local authority can only use RIPA authorisations for the purpose of preventing or detecting crime or of preventing disorder. For directed surveillance to be authorised, it must be for the purpose of preventing or detecting conduct which constitutes/corresponds to a criminal offence punishable at least 6 months imprisonment (or an offence under section 146, 147, or 147A of the Licensing act 2003).**

- be satisfied that the directed surveillance is **necessary** in the circumstances of the particular case.

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

- be satisfied that the possibility of collateral intrusion 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.

If there is an alternative practicable means of carrying out the surveillance, which is less intrusive, then the surveillance is neither necessary nor proportionate and should not be authorised. The least intrusive method should be used

Additional Factors when Authorising a CHIS

In addition, when authorising the conduct or use of a CHIS the Authorising Officer must

- be satisfied that the **conduct** and/or **use** of the CHIS is proportionate to what is sought to be achieved.

- be satisfied that **appropriate arrangements** are in place for the management and oversight of the CHIS.

- consider the likely degree of intrusion of all those potentially effected.

- consider any adverse impact on community confidence that may result from the use or conduct or the information obtained.

- ensure **records** contain statutory particulars and are not available except on a need to know basis.

- ensure that authorisations relating to the use of a juvenile CHIS are only for one month at a time.

- be satisfied that a full risk assessment has been undertaken.

9.6 The role of Senior Responsible Officer (SRO) is undertaken by the Service Director: Legal and Community and Monitoring Officer. The role of RIPA Co-ordinating Officer is undertaken by the Monitoring Officer Technical Support & PA to Service Director: Legal and Community.

The SRO is responsible for:

- the integrity of the process in place within the public authority for the management of CHIS and Directed Surveillance;

- compliance with Part 2 of the Act and with the Codes;

- oversight of the reporting of errors to the relevant oversight Commissioner and the identification of both the cause(s) of errors and the implementation of processes to minimise repetition of errors;

- engagement with the OSC inspectors when they conduct their inspections, where applicable; and

- where necessary, oversight of the implementation of post-inspection action plans approved by the relevant oversight Commissioner.

9.7 The role of CHIS Handler will be allocated to either one of the Service Director: Place, Service Director: Customers, or Service Director: Regulatory, depending which directorate is using the CHIS. The CHIS Controller will be allocated to one of the other two heads of service by the Chief Executive.

The CHIS Handler is responsible for:

- dealing with the CHIS on behalf of the Council;

- directing the day to day activities of the CHIS;

- recording the information supplied by the CHIS; and

- monitoring the CHIS's security and welfare.

The CHIS Controller is responsible for management and supervision of the CHIS Handler, and general oversight of the use of CHIS.

10. WORKING WITH / THROUGH OTHER AGENCIES

10.1 The Council may work in conjunction with other agencies to carry out covert surveillance and to use CHIS's, eg police, DWP, Inland Revenue (but does not include RSLs). It is not necessary for each party to complete its own form of authorisation, and the Council can rely upon a duly authorised form completed by another agency providing that the Authorising Officer is made aware and it has been approved by the Magistrates' Court if required. If another agency chooses to rely on a RIPA authorisation from this Council the Authorising Officer must be made aware.

10.2 A copy of another agency's authorisation should be obtained and copies kept in the same manner as an authorisation granted by the Council. Officers should also ensure that review and renewal dates are noted and that copies of the appropriate forms are also obtained and kept appropriately.

10.3 In the event that a member of staff has concerns that an authorisation, Magistrates' Court approval, review, or renewal completed by a partner agency does not comply with the law, codes of practice, or agreed arrangements for surveillance, they should refer the matter to an Authorising Officer of the Council for further action as necessary.

10.4 When another agency (e.g. the Police, Inland Revenue 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.

11. RECORD MANAGEMENT

11.1 The Council must keep a detailed record of all authorisations, Magistrates' Court approvals, reviews, renewals, and cancellations. Copies of all authorisations, Magistrates' Court approvals, records of oral authorisations, reviews, renewals, cancellations and refusals must be kept in a central register held by an Authorised Officer. In addition all original authorisations, records of oral authorisations, Magistrates' Court approvals, reviews, renewals, cancellations, refusals and other relevant documents must be sent to the RIPA Co-ordinating Officer, who maintains the central RIPA log (record of authorisations and rejections).

11.2 All information obtained during directed surveillance should be recorded in a surveillance log. This should be in a format that gives an accurate and suitably detailed account of the events observed and conversations heard at particular times.

11.3 Copies of all authorisations, records of oral authorisations, Magistrates' Court approvals, reviews, renewals, cancellations and refusals should be kept for a period of 5 years after the conclusion of any Court proceedings arising for which the surveillance or use of the CHIS was relevant. If it is believed that the records could be relevant to pending or future criminal proceedings, the officer in charge of the investigation shall confirm that they should be retained for a suitable further period, subject to any subsequent review, prior to the expiry of the five year period. This decision must be notified to the Service Director: Legal and Community.

11.4 Records maintained in the Directorates and Centrally

11.4.1 Generally, all material (in whatever media) produced or obtained during the course of investigations subject to RIPA authorisation (whether authorised or not), should be processed, stored and destroyed in accordance with the requirements of the Data Protection Act 2018, General Data Protection Regulation (GDPR) (EU) 2016/679, the Freedom of Information Act 2000 and any other legal requirements, including those of confidentiality and the Council's policies and procedures regarding document retention. The following paragraphs give guidance on some specific situations, but advice should be sought from the Service Director: Legal and Community, or the Data Protection and Freedom of Information Officer where appropriate. All documents must be retained securely and electronic copies of documents must be password protected.

11.4.2 Copies of the following documents must be retained securely in the departments. Original documents must be sent to the Monitoring Officer within 5 working days. They should be submitted in a sealed envelope marked "Confidential RIPA forms".

- The application and the authorisation together with any supplementary documentation and notification of the approval given by the Authorising Officer;
- The application to the Magistrates' Court and any relevant approval/court order;

- 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;
- Any renewal of an authorisation, together with the supporting documentation submitted when the renewal was requested and Magistrates' Court approval;
- The date and time when any instruction was given by the Authorising Officer.
- An electronic log is maintained centrally on a restricted public folder within G/drive. The Log is kept in a password-protected Excel spreadsheet, located in drive G/*RIPA 2000/ RIPA Log.* Only Authorising Officers can view it.
- The Council shall retain records for a period of at least 6 years from the ending of the authorisation. The Investigatory Powers Commissioner's Office (IPCO) can review the Council's policies and procedures and individual authorisations. The IPCO usually provide notice before an inspection, but can arrive unannounced.

  Copies of authorisations, renewals and cancellations are discoverable in legal proceedings. If proper records are not maintained, evidence gathered may be inadmissible.

11.5 Records Relating to the CHIS

11.5.1 All information obtained by the CHIS and by the officer responsible for recording the use of the CHIS should be recorded by means of a daily log. This should be in a format that gives an accurate and suitably detailed account of the events observed and conversations heard at particular times.

11.5.2 All information recorded in respect of authorisations, surveillance or the use of CHIS must only be disclosed for the purposes for which it was gathered at the time or for use in any future civil or criminal proceedings brought by or against the Council.

11.5.3 Records which reveal the name(s) of the CHIS should only be disclosed to persons to the extent that there is a need for access to them; if legally necessary; or if ordered by any Court.

11.5.4 When it is intended to employ a CHIS a record must be kept that records all the detail specified in Appendix 2. The officer in charge of maintaining a record of the use of each CHIS should record all these details. The way these records are kept is designed to try to keep the CHIS safe from discovery by the subjects and safe from any harm which could result from their disclosure and also to keep in the open any money or other benefits paid to a CHIS who is not an employee officer of an authorising body.

12. RECORDED MATERIAL OBTAINED DURING INVESTIGATIONS

12.1 Where recorded material (in any form or media) is obtained during the course of an investigation which might be relevant to that investigation, or another investigation, or to pending or future civil or criminal proceedings, then it should **not** be destroyed, but retained in accordance with the requirements of the Data Protection Act 2018, General Data Protection Regulation (GDPR) (EU) 2016/679, the Freedom of Information Act 2000, and any other legal

requirements, including those of confidentiality, and the Council's policies and procedures regarding document retention. Advice should be sought from the Monitoring Officer or the Information and Records Manager.

12.2 Where recorded material is obtained, which is not related to a criminal or other investigation or to any person who is the subject of the investigation, and there is no reason to suspect that it will be relevant to any future civil or criminal proceedings, it should be destroyed immediately.

12.3 Recorded Material obtained in the course of an investigation may be used in connection with investigations other than the one that the relevant authorisation was issued for. However, the use or disclosure of such material outside the Council, unless directed by any court order, should only be considered in exceptional circumstances and in accordance with advice from the Monitoring Officer.

12.4 Where recorded material obtained is of a confidential nature, then the following additional precautions should be taken:

- Confidential recorded material should not be retained or copied unless it is necessary for a specified purpose;
- Confidential recorded material should only be disseminated in accordance with legal advice that it is necessary to do so for a specific purpose;
- Confidential recorded material which is retained should be marked with a warning of its confidential nature. Safeguards should be put in place to ensure that such recorded material does not come into the possession of any person where to do so might prejudice the outcome of any civil or criminal proceedings;
- Confidential recorded material should be destroyed as soon possible after it is used for the specified purpose.
- Confidential recorded material should be made available for the Office of Surveillance Commissioners at the time of any Inspection.

12.5 If there is any doubt as to whether material is of a confidential nature, advice should be sought from the Monitoring Officer.

12.6 The Authorising Officer must ascertain what material has been obtained by the use of directed surveillance. The Authorising Officer should comment on the material and how it is to be managed or used thereafter. If the matter is not proceeding to a prosecution, the Authorising Officer must be satisfied that any material has been securely destroyed.

13. SOCIAL NETWORKING SITES

13.1 Where privacy settings are available but not applied the data available on Social Networking Sites may be considered 'open source' and an authorisation is not usually required.

13.2 Repeat viewing of 'open source' sites, however, may constitute directed surveillance on a case by case basis and this should be borne in mind e.g. if someone is being monitored through, for example, their Facebook profile for a period of time and a record of the information is kept for later analysis, this is likely to require a RIPA authorisation for directed surveillance.

13.3 To avoid the potential for inadvertent or inappropriate use of social network sites in investigative and enforcement roles, Council Officers should be mindful of any relevant guidance and the Council's separate policy regarding the use of Social Networking Sites: Conduct of Investigations.

13.4 The Home Office Revised Code of Practice on Covert Surveillance and Property Interference, published in August 2018, provides the following guidance in relation to online covert activity:

'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 in 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 following guidance is intended to assist public authorities in identifying when such authorisations may be appropriate.

The internet may be used for intelligence gathering and/or as a surveillance tool. Where online monitoring or investigation is conducted covertly for the purpose of a specific investigation or operation and is likely to result in the obtaining of private information about a person or group, an authorisation for directed surveillance should be considered, as set out elsewhere in this code. Where a person acting on behalf of a public authority is intending to engage with others online without disclosing his or her identity, a CHIS authorisation may be needed (paragraphs 4.10 to 4.16 of the Covert Human Intelligence Sources code of practice provide detail on where a CHIS authorisation may be available for online activity).

In deciding whether online surveillance should be regarded as covert, consideration should be given to the likelihood of the subject(s) knowing that the surveillance is or may be taking place. Use of the internet itself may be considered as adopting a surveillance technique calculated to ensure that the subject is unaware of it, even if no further steps are taken to conceal the activity. Conversely, where a public authority has taken reasonable steps to inform the public or particular individuals that the surveillance is or may be taking place, the activity may be regarded as overt and a directed surveillance authorisation will not normally be available.

As set out below, depending on the nature of the online platform, there may be a reduced expectation of privacy where information relating to a person or group of people is made openly available within the public domain, however in some circumstances privacy implications still apply. This is because the intention when making such information available was not for it to be used for a covert purpose such as investigative activity. This is regardless of whether a user of a website or social media platform has sought to protect such information by restricting its access by activating privacy settings.

Where information about an individual is placed on a publicly accessible database, for example the telephone directory or Companies House, which is commonly used and known to be accessible to all, they are unlikely to have any reasonable expectation of privacy over the monitoring by public authorities of that information. Individuals who post information on social media networks and other websites whose purpose is to communicate messages to a wide audience are also less likely to hold a reasonable expectation of privacy in relation to that information.

Whether a public authority interferes with a person's private life includes a consideration of the nature of the public authority's activity in relation to that information. Simple reconnaissance of such sites (i.e. preliminary examination with a view to establishing whether the site or its contents are of interest) is unlikely to interfere with a person's reasonably held expectation of privacy and therefore is not likely to require a directed surveillance authorisation. But where a public authority is systematically collecting and recording information about a particular person or group, a directed surveillance authorisation should be considered. These considerations apply regardless of when the information was shared online.'

14. TRAINING

14.1 Training on RIPA and the procedures set out in this policy document will be given or authorised by the Service Director: Legal and Community. Any officer who wishes to undertake surveillance or employ a CHIS and all Authorising Officers must receive and maintain suitable training before signing any RIPA authorisations.

14.2 A Central Register of all officers who have received training on RIPA will be maintained by the Service Director: Legal and Community.

14.3 As part of the periodic review of this Policy and Procedures the Monitoring Officer will determine any ongoing training needs both for Authorising Officers and applicant officers. Refresher courses will be held as necessary.

14.4 The responsibility for ensuring that staff receive appropriate training in connection with RIPA lies with Service Directors.

14.5 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 familiarising 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 minimise collateral intrusion.

14.6 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.

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

14.8 The Monitoring Officer will invite pertinent officers to a biannual forum to discuss RIPA and issues relating to enforcement. The forum should aim to benchmark best practice.

15. ELECTED MEMBER INVOLVEMENT

15.1 Two new Codes of Practice came into effect on 6 April 2010:

- Regulation of Investigatory Powers (Covert Human Intelligence Source: Code of Practice) Order 2010
- Regulation of Investigatory Powers (Covert Surveillance and Property Interference: Code of Practice) Order 2010

15.2 The Codes of Practice state that elected members should:

- Set the RIPA policy at least once a year
- Review the local authority's use of RIPA
- Consider internal reports on the use of RIPA on at least a quarterly basis

15.3 The Terms of Reference for Cabinet in the Council's Constitution state that Cabinet is:

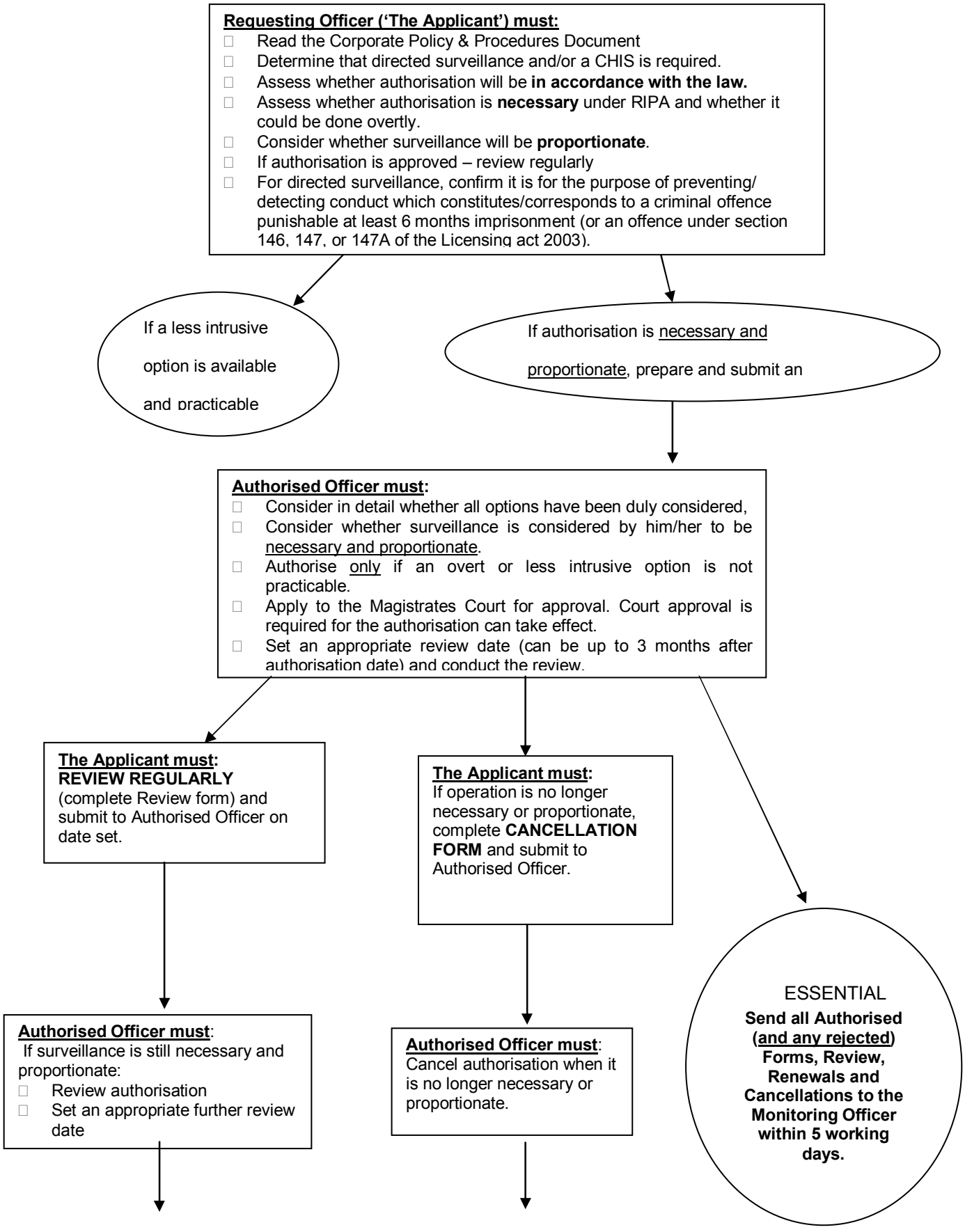
"To prepare and agree to implement policies and strategies other than those reserved to Council."

The setting of the RIPA policy annually is therefore a role for Cabinet. The Partnerships Scrutiny Sub Committee will consider the Policy annually and make recommendations to Cabinet.

15.4 The requirement for members to review the local authority's use of RIPA and consider internal reports on the use of RIPA on at least a quarterly basis is to be undertaken by the Overview and Scrutiny Committee in accordance with the terms of reference for that Committee contained in the Council's constitution.

APPENDIX A

FLOW CHART OF RIPA PROCESS

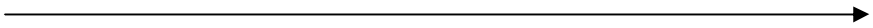


- Send all Quarterly Returns to MO

- Regulation of Investigatory Powers (Covert Human Intelligence Source: Code of Practice) Order 2010
- Regulation of Investigatory Powers (Covert Surveillance and Property Interference: Code of Practice) Order 2010

- The Codes of Practice state that elected members should:

    - Set the RIPA policy at least once a year
    - Review the local authority's use of RIPA
    - Consider internal reports on the use of RIPA on at least a quarterly basis



APPENDIX B

AUTHORISING OFFICERS AND RESPONSIBLE OFFICERS

RIPA Authorising Officers	Chief Executive, or in his absence the Deputy Chief Executive, Service Director: Place, Service Director: Customers, Service Director: Regulatory
Authorising operations where confidential information may be obtained	Chief Executive only
CHIS Authorising Officer	Chief Executive only
CHIS Controller/Handler	Service Director: Place Service Director: Customers Service Director: Regulatory
Senior Responsible Officer	Service Director: Legal and Community and Monitoring Officer
RIPA Co-ordinating Officer	PA to Service Director: Legal and Community

Please note:

- Where use of a CHIS is authorised, the head of the directorate carrying out the activity shall usually act as the CHIS Handler, with the CHIS Controller role being allocated by the Chief Executive.
- Authorising Officers must be “an assistant chief officer or investigations manager” or above.
- The Authorising Officers should not be directly involved in the investigation.