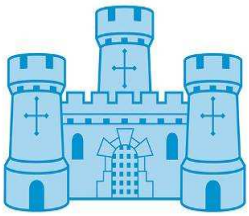


NEWCASTLE·UNDER·LYME
BOROUGH COUNCIL

HUMAN RIGHTS ACT 1998

REGULATION OF INVESTIGATORY POWERS ACT 2000 (RIPA) AS AMENDED

POLICY AND GUIDANCE ON USE OF RIPA

UPDATED MARCH 2013

INTRODUCTION

The purpose of this policy and associated procedures is to ensure compliance with the requirements of the Regulation of Investigatory Powers Act (RIPA) as amended from 1st November 2012 by the Protection of Freedoms Act 2012.

This Policy takes account of the primary and secondary legislation, Codes of Practice and Guidance issued by the Home Office.

The Senior Responsible Officer (SRO) for the purposes of this policy is the Head of Central Services. The responsibilities of the SRO are set out in the revised (2010) Home Office "Covert Surveillance and Property Interference" Code of Practice paragraphs 3.28 and 3.29:

3.28 It is considered good practice that within every relevant public authority, a Senior Responsible Officer should be responsible for:

- The integrity of the process in place within the public authority to authorise directed surveillance
- Compliance with Part II of the 2000 Act (in relation to covert surveillance that is likely to result in the obtaining of private information) and with the 2010 Code of Practice
- Engagement with the Commissioners and inspectors when they conduct their inspections; and
- Where necessary, overseeing the implementation of any post-inspection action plans recommended or approved by a Commissioner.

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

Although no identical provisions are contained in the corresponding "Covert Human Intelligence Sources" Code of Practice, the SRO will also fulfil similar tasks for the use of Covert Human Intelligence Sources (CHIS).

In all cases, officers considering any operations which might or will necessitate a RIPA authorisation should firstly consult the Senior Responsible Officer who will advise accordingly.

LOCAL AUTHORITY USE OF RIPA ('the 2000 Act')

The Borough Council will only carry out covert surveillance where such action is justified and endeavours to keep such surveillance to a minimum. Any officer intending to acquire data covertly will only do so if the evidence or intelligence sought cannot be obtained by any overt other means.

The existing regulatory framework

The 2000 Act sets out a regulatory framework for the use of covert investigatory techniques by public authorities. It does not provide any powers to carry out covert activities. If such activities are conducted by Council officers, then RIPA regulates them in a manner that is compatible with the European Convention on Human Rights (ECHR), particularly Article 8 - the right to respect for private and family life. Interference with that right could only be on the basis of a specified ground and 'in accordance with the law'. Until RIPA was introduced, there was no statutory basis for covert surveillance in England and Wales.

RIPA enables local authorities to interfere with private and family life protected by Article 8 of the ECHR provided it is necessary and proportionate to do so. This may be necessary to enable the Borough Council to effectively investigate and obtain evidence in a range of core regulatory functions that they have a statutory duty to enforce and covers the use of covert surveillance for test purchasing and other enforcement activities. However, powers are now limited under the Protection of Freedoms Act 2012.

The 2000 Act allows three types of covert surveillance - directed (DS), intrusive (IS) and covert human intelligence sources (CHIS)), but limits local authorities to using only DS and CHIS, together with the ability to obtain telecommunications data (but not content) – and **only** for the purpose of preventing or detecting crime or preventing disorder. Local authorities have no power to carry out intrusive surveillance. DS, IS and CHIS are explained later in this document.

Use of these techniques has to be authorised internally by an authorising officer (see below). Covert surveillance can only be used where it is considered **necessary** (e.g. to investigate a suspected crime or disorder) and **proportionate** (e.g. balancing the seriousness of the intrusion into privacy against the seriousness of the offence and whether the information can be obtained by other means).

Local authorities are no longer able to use directed surveillance in some cases where it was previously authorised. For this Council, this included flytipping and taxi plying for hire operations. But this does not mean that it will not be possible to investigate these areas with a view to stopping offending behaviour. The "Covert Surveillance and Property Interference" Code of Practice on covert surveillance makes it clear that routine patrols, observations at trouble 'hotspots', immediate response to events and overt use of CCTV are all techniques which do not require RIPA authorisation (see paras 2.21 et seq).

Local authorities are required to obtain judicial approval prior to using covert techniques. Local authority authorisations under RIPA will only be given effect once an order has been granted by a Justice of the Peace.

Additionally, local authority use of directed surveillance under RIPA will be limited to the investigation of crimes which attract a maximum sentence of six months (or longer) custody, with the exception of certain offences relating to the sale of alcohol and other age restricted products to persons who are under-age.

Surveillance Techniques

Surveillance can be either 'directed' or 'intrusive'. Brief descriptions of these terms are given below. However, local authorities do not have the power to carry out intrusive surveillance.

Surveillance:

Surveillance includes the following (section 48(2) RIPA):

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

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

(c) surveillance by or with the assistance of a surveillance device.

Directed surveillance:

(a) is covert – i.e. done in such a way as to be hidden from the subject of investigation

(b) is likely to result in private information about the subject or any other person (i.e. information relating to a person's private or family life, his/her home or correspondence (whether or not that person is specifically targeted for the purposes of an investigation)).

Intrusive surveillance:

Intrusive surveillance is defined in section 26(3) of the 2000 Act as covert surveillance that:

(a) is carried out in relation to anything taking place on any residential premises or in any private vehicle; and

(b) involves the presence of an individual on the premises or in the vehicle or is carried out by means of a surveillance device (cameras, tape recorders etc.)

BUT surveillance carried out in relation to residential premises by use of a device (i.e. a camera) which is not in or on the premises is not 'intrusive' (although it will be 'directed') unless it is of the same quality of information as would be obtained if the equipment was situated in the premises.

Behaviour which is <u>not</u> covert surveillance (i.e. it is overt):

- a visit by an authorised member of staff who announces the reason for their visit and requests entry to the premises
- any information obtained as a result of questions to the resident
- any information obtained as a result of observation in the part of the premises to which the officer is invited
- any information obtained as a result of a request to make an inspection
- the recording of a telephone conversation with the agreement of the other party
- entering on to residential premises to take action to address an immediate nuisance is not covert surveillance.

If there is any doubt as to whether an activity is or is not covert surveillance, a precautionary approach should be adopted, legal advice should be sought, and the activity treated as covert surveillance.

<u>Use of Covert Human Intelligence Sources (CHIS)</u>

A person is a covert human intelligence source if he or she:

a) Establishes or maintains a relationship (which can be a personal relationship or a business relationship, e.g. a contract) with a person either to use the relationship to obtain information or to disclose information obtained as a result of such a relationship

b) The surveillance is covert if and only if it is carried on in a manner calculated to ensure that one of the parties to the relationship is unaware of the purpose of that relationship.

The circumstances in which the Council may be considered to be using a covert human intelligence source is where a neighbour is requested to provide information about a neighbour and it is information obtained not by personal observation as in the case of neighbour nuisance, but is information obtained

through conversation with the neighbour under investigation such as personal relationships. This means that asking a neighbour for information regarding who is living in a property and the relationship between the parties would be using that person as a covert human intelligence source, which would need special authorisation.

Asking a neighbour to keep records of nuisance suffered by the neighbour would not be using a covert human intelligence source because the neighbour would not be relying on a relationship with the person under investigation to obtain information.

Although it is not likely to occur very often, the Borough Council recognises that it may occasionally have to undertake the use of CHIS activity. As with authorisations for directed surveillance, judicial approval is required before a CHIS can be used.

Any officer contemplating the use of a CHIS should immediately consult the Senior Responsible Officer.

Interception of Communications and Access to Communications Data

Communications data means:

- Who made the communication and when and where they made it

but NOT the content.

It includes the manner in which, and by what method, a person or device communicates with another person or device.

Authorisation can only be given if it is necessary for the purpose of preventing or detecting crime or of preventing disorder.

As an employer, the Council may intercept employees' emails (when sent or received on a Council computer or other electronic device) with the consent of the employee. Consent is not however needed where the purpose is to detect and prevent crime or unauthorised use of the email or internet system.

Under the Regulation of Investigatory Powers (Communications Data) Order 2010 (S.I. 2010/480), a Director, Head of Service, Service Manager or equivalent can authorise access to communications data. Examples of such data are:

- Itemised telephone call records and connections to internet services

- Information about the connection, disconnection and reconnection of services

- Records of registered, recorded or special delivery postal items.

Examples of subscriber information are:

- Who is the subscriber of a particular phone number or email account
- What services a subscriber or account holder has subscribed to, including payment methods
- Addresses for installation and billing.

The use of these powers is subject to a Code of Practice issued by the Home Office. This includes information about:

a) the form and content of an application

b) the content of an authorisation or notice

c) the validity period for an authorisation or notice

d) the records to be kept.

RIPA provides two different ways of obtaining communications data.

1. An authorisation given by a designated officer. This allows the Council to find out the information itself

2. By a notice served on the service provider which compels it to provide the information.

Any authorisation under section 22 of RIPA for access to communications data will not take effect until approved by a Magistrate in accordance with section 23A.

The tests for necessity and proportionality apply in the same way as for directed surveillance – see below.

AUTHORISATION OF COVERT SURVEILLANCE

The Borough Council is a 'relevant authority' under Section 30 and Schedule 1 (as amended by the Regulation of Investigatory Powers (Directed Surveillance and Covert Human Intelligence Sources) Order 2010 (S.I. 2010/521)).

'Authorising Officers' must hold an office, rank or position prescribed by the above order, and these positions are:

- Director
- Head of Service
- Service manager or equivalent.

The Council's Scheme of Delegations specifies the Authorising Officers for the Borough Council as:

Chief Executive
Executive Director (Resources and Support Services)
Executive Director (Regeneration and Development Services)
Executive Director (Operational Services).

Where a covert surveillance operation may result in the obtaining of private information, the Authorising Officer must be the Chief Executive or (in his/her absence, the person acting as the Chief Executive).

Roles of the Applicant and Authorising Officer –
these roles are NOT the same
(para. 104, OSC Procedures and guidance)

The role of the applicant is to present the facts of the application for covert surveillance:

- the crime to be investigated;
- the reason why it is proposed to conduct the investigation covertly;
- what covert tactics are requested and why; who the covert surveillance will be focused on; who else may be affected by it; and
- how it is intended to conduct covert surveillance.

To assist the authorising officer's assessment of proportionality, the applicant should provide facts and evidence but it is not the role of the applicant to assert that it is necessary and proportionate – that is the responsibility of the authorising officer. However, the applicant should address and consider why he/she considers that the authorisation being applied for is necessary and proportionate.

The authorising officer's statement should preferably be completed in handwriting as a personal contemporaneous record of the thinking which justified the authorisation.

The tests of necessity and proportionality for Directed Surveillance

Necessity

The action must be **necessary** and the only 'necessary' reason available to a local authority is for the prevention or detection of crime or the prevention of disorder. This is the starting point for determining necessity, but it is further limited by Regulation 7A of the Regulation of Investigatory Powers (Directed Surveillance and Covert Human Intelligence Sources) (Amendment) Order 2012 – S.I. 2012/1500.

Accordingly, any Directed Surveillance must be for the purpose of preventing or detecting conduct which:

(i) constitutes one or more criminal offences; or

(ii) is, or corresponds to, any conduct which, if it all took place in England and Wales, would constitute one or more criminal offences.

AND

The offence(s) must be:

a) An offence which is punishable, whether on summary conviction or on indictment, by a maximum term of at least 6 months imprisonment; or

b) An offence under:

(i) Section 146 of the Licensing Act 2003 – sale of alcohol to children

(ii) Section 147 of the Licensing Act 2003 – allowing the sale of alcohol to children

(iii) Section 147A of the Licensing Act 2003 – persistently selling alcohol to children

(iv) Section 7 of the Children and Young Persons Act 1933 – sale of tobacco etc. to persons under 18.

Proportionality

The surveillance is **proportionate** to what is sought to be achieved by carrying out the surveillance e.g. impairs as little as possible the rights and freedoms (of the individual concerned and of innocent third parties); is carefully designed to meet the objectives in question; is not arbitrary, unfair or based on irrational considerations.

The grant of authorisation should indicate that serious consideration has been given to the above points. The authorising officer's statement should include a full account of what is being authorised and how and why the authorising officer is satisfied that the operation is necessary and proportionate. The authorising officer's statement should spell out the five 'W's:

- **WHOM** the surveillance is directed against
- **WHAT** surveillance/activity is sanctioned
- **WHEN** and
- **WHERE** the surveillance/activity will take place; and
- **WHY** it is necessary.

An authorising officer should not normally be responsible for authorising operations in which they are directly involved, although it is recognised that this may sometimes be unavoidable. Where an authorising officer authorises such an investigation or operation, the central record of authorisations should highlight this.

Before authorising applications, the authorising officer should also take into account the risk of obtaining private information about persons who are not subjects of the surveillance or property interference activity (collateral intrusion).

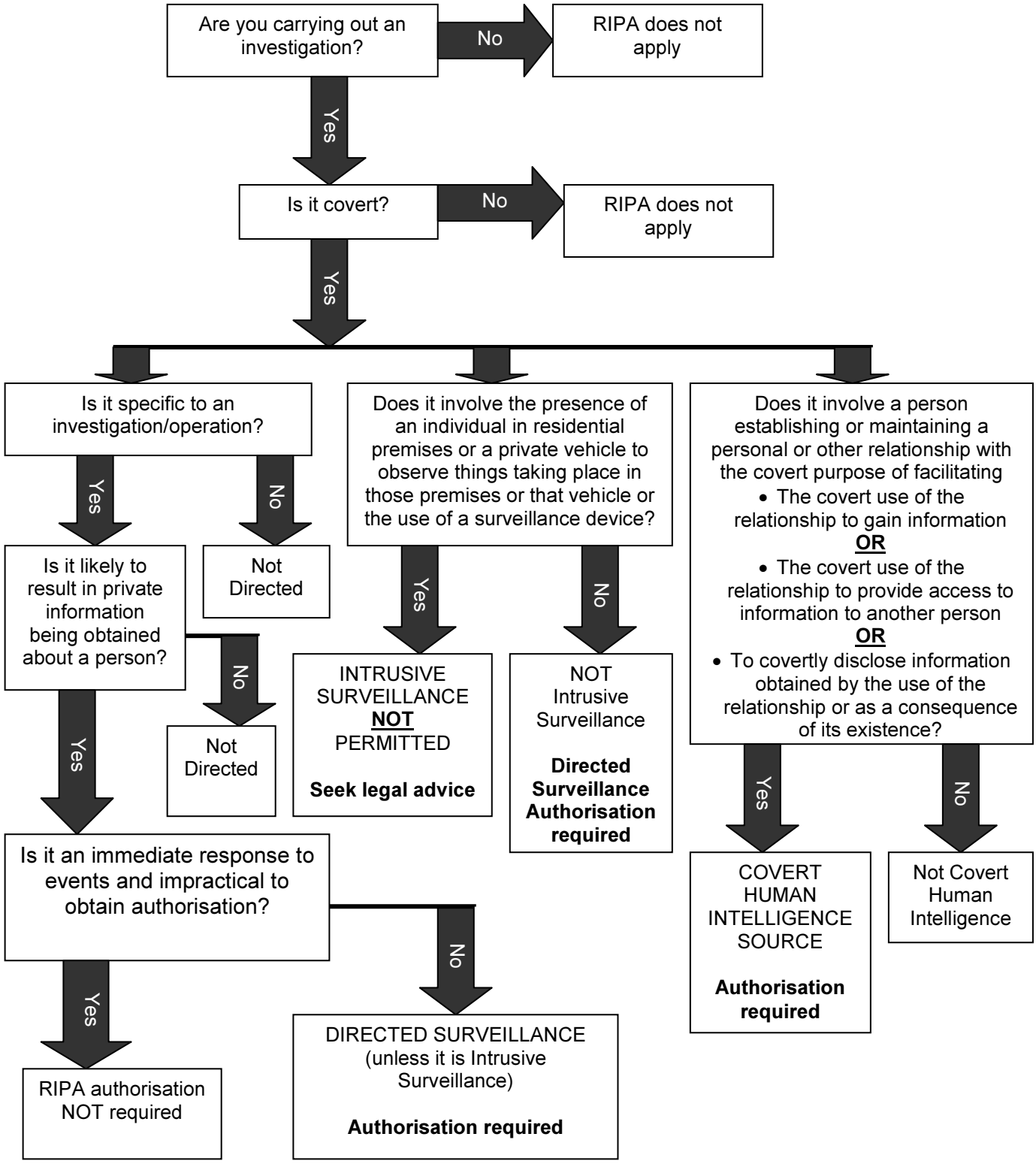
At the point in any investigation where any activity is being contemplated which might amount to covert surveillance such as:

- following someone without their knowledge

- taking photographs of someone without their knowledge

- recording a telephone conversation without the agreement of the other party.

Officers need to consider whether the activities contemplated are covert surveillance and therefore require authorisation. The flowchart below is a guide as to whether authorisation may be needed or not.


Are you carrying out an investigation?
No
RIPA does not apply
Yes
Is it covert?
No
RIPA does not apply
Yes
Is it specific to an investigation/operation?
Yes
No
Not Directed
Is it likely to result in private information being obtained about a person?
No
Not Directed
Yes
Is it an immediate response to events and impractical to obtain authorisation?
Yes
RIPA authorisation NOT required
No
DIRECTED SURVEILLANCE (unless it is Intrusive Surveillance)
Authorisation required
Does it involve the presence of an individual in residential premises or a private vehicle to observe things taking place in those premises or that vehicle or the use of a surveillance device?
Yes
INTRUSIVE SURVEILLANCE NOT PERMITTED
Seek legal advice
No
NOT Intrusive Surveillance
Directed Surveillance Authorisation required
Does it involve a person establishing or maintaining a personal or other relationship with the covert purpose of facilitating
• The covert use of the relationship to gain information
OR
• The covert use of the relationship to provide access to information to another person
OR
• To covertly disclose information obtained by the use of the relationship or as a consequence of its existence?
Yes
COVERT HUMAN INTELLIGENCE SOURCE
Authorisation required
No
Not Covert Human Intelligence

If, following the flowchart and Policy, it appears to an investigating officer that an authorisation for either DS or CHIS is required, the appropriate application must be completed on the model form (Appendix A) and submitted to the Authorising Officer.

DS authorisations last for 3 months. CHIS authorisations last for 12 months unless the source is aged under 18 in which case they last for one month. Any can be renewed before they expire by an authorising officer.

It must be recognised that any RIPA authorisation can only be granted for those specified periods of time, even if the surveillance is due to take place on the same or next day, or last for a very short time. All authorisations should be monitored closely by the Authorising Officer to ensure that they are cancelled as soon as they are no longer necessary or proportionate (or in the case of a CHIS, the additional requirements for handler and controller are no longer in place). This is especially important in any short term operations.

Directed Surveillance Judicial Approval

Once the authorisation has been completed, an application must be made to a single Magistrate under s.32A of the 2000 Act. To bring the directed surveillance authorisation into force, the Magistrate must be satisfied:

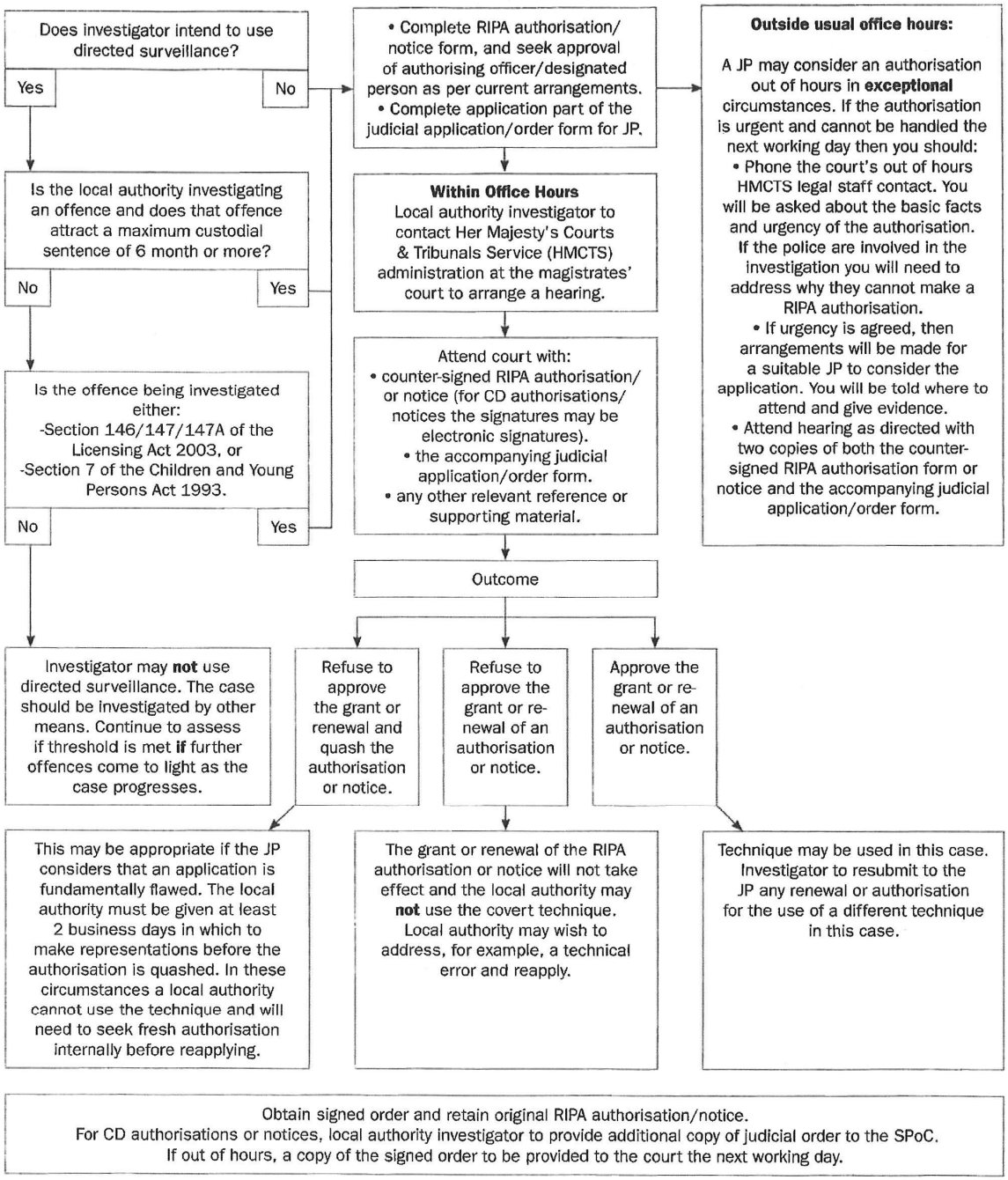
a) That at the time of the grant (by the authorising officer), there were reasonable grounds for believing the authorisation was necessary and proportionate

b) The Authorising Officer was properly designated; and

c) That the authorisation is still (i.e. at the time of the application) necessary and proportionate.

The order form for submission to the Magistrate is attached at Appendix B.

A flowchart setting out these steps is set out below:


Does investigator intend to use directed surveillance?
Yes
No
Is the local authority investigating an offence and does that offence attract a maximum custodial sentence of 6 month or more?
No
Yes
Is the offence being investigated either:
-Section 146/147/147A of the Licensing Act 2003, or
-Section 7 of the Children and Young Persons Act 1993.
No
Yes
Investigator may not use directed surveillance. The case should be investigated by other means. Continue to assess if threshold is met if further offences come to light as the case progresses.
• Complete RIPA authorisation/ notice form, and seek approval of authorising officer/designated person as per current arrangements.
• Complete application part of the judicial application/order form for JP.
Within Office Hours
Local authority investigator to contact Her Majesty's Courts & Tribunals Service (HMCTS) administration at the magistrates' court to arrange a hearing.
Attend court with:
• counter-signed RIPA authorisation/ or notice (for CD authorisations/ notices the signatures may be electronic signatures).
• the accompanying judicial application/order form.
• any other relevant reference or supporting material.
Outcome
Refuse to approve the grant or renewal and quash the authorisation or notice.
Refuse to approve the grant or re-newal of an authorisation or notice.
Approve the grant or re-newal of an authorisation or notice.
This may be appropriate if the JP considers that an application is fundamentally flawed. The local authority must be given at least 2 business days in which to make representations before the authorisation is quashed. In these circumstances a local authority cannot use the technique and will need to seek fresh authorisation internally before reapplying.
The grant or renewal of the RIPA authorisation or notice will not take effect and the local authority may not use the covert technique. Local authority may wish to address, for example, a technical error and reapply.
Technique may be used in this case. Investigator to resubmit to the JP any renewal or authorisation for the use of a different technique in this case.
Outside usual office hours:
A JP may consider an authorisation out of hours in exceptional circumstances. If the authorisation is urgent and cannot be handled the next working day then you should:
• Phone the court's out of hours HMCTS legal staff contact. You will be asked about the basic facts and urgency of the authorisation. If the police are involved in the investigation you will need to address why they cannot make a RIPA authorisation.
• If urgency is agreed, then arrangements will be made for a suitable JP to consider the application. You will be told where to attend and give evidence.
• Attend hearing as directed with two copies of both the counter-signed RIPA authorisation form or notice and the accompanying judicial application/order form.
Obtain signed order and retain original RIPA authorisation/notice.
For CD authorisations or notices, local authority investigator to provide additional copy of judicial order to the SPoC.
If out of hours, a copy of the signed order to be provided to the court the next working day.

Directed Surveillance Post Authorisation Activity

Once an authorisation has been approved by the Magistrate, then officers undertaking the investigation will need to carry out the following steps:

1) keep a log in the agreed format of all actions undertaken during the surveillance (controlled stationery must be obtained for this purpose)

2) all entries in the log must include times, dates, persons present and be signed

3) a similar log will need to be kept for any photographs, video and/or sound recordings taken

4) authorising officers must ensure compliance with the appropriate data protection requirements and any relevant codes of practice

5) a centrally retrievable record of all authorisations must be kept and regularly updated whenever an authorisation is granted, renewed or cancelled. The record is made available to the relevant Commissioner or an Inspector from the OSC upon request. The record is kept securely in the office of the Head of Central Services. However, departments may securely keep their own record of authorisations granted but the original must be placed on the central record. Records should be kept for at least 3 years from the end of the authorisation

6) authorisations must be uniquely numbered

7) where it is envisaged during the course of an investigation that specific equipment will be used, e.g. camera/sound recording equipment, the request for authorisation should specifically refer to this and be approved in the authorisation

8) where the product of surveillance could be relevant to pending or future proceedings, it should be retained in accordance with established disclosure requirements for a suitable further period, commensurate to any subsequent review.

Covert Human Intelligence Source (CHIS)

Authorisation levels are the same as for directed surveillance, i.e. an officer of a relevant authority.

Under Section 30 and Schedule 1 (as amended by the Regulation of Investigatory Powers (Directed Surveillance and Covert Human Intelligence Sources) Order 2010 (S.I. 2010/521), the officer must hold an office, rank or position prescribed by this Order.

Authorisation must not be granted unless the Authorising Officer believes it is **necessary** i.e. for the purpose of preventing or detecting crime or of preventing disorder, and **proportionate** to what is sought to be achieved by carrying out the surveillance. As with Directed Surveillance, no other grounds are available.

A CHIS can be used for any purpose of preventing or detecting crime or of preventing disorder. There are no limitations on the type of crime.

With CHIS, there are additional requirements for authorisation. There must be arrangements in place for ensuring (section 29(5) that:

(a) someone (holding the required office, rank or position for authorising surveillance) has day to day responsibility for dealing with the source and for his/her security and welfare ('handler')

(b) another has general oversight of the use made of the source ('controller')

(c) someone has responsibility for maintaining a record of the use made of the source

(d) the records contain particulars specified by the Secretary of State in the Regulation of Investigatory Powers (Source Records) Regulations 2000 S.I. 2000/2725.

Where the source acts for more than one public authority, only one authority must have responsibility for each of (a) to (d) above.

Additionally, the authorisation must specify:

- The conduct or use of the source
- The person he/she is used against
- The purpose of the investigation/operation involved.

The Secretary of State can prohibit certain conduct or uses of covert sources altogether or impose extra requirements before authorisations are granted.

Under the Regulation of Investigatory Powers (Juveniles) Order 2000 S.I. 2000/2793 - a source under 16 cannot be used to obtain information about his/her parent or anyone having parental responsibility.

Where a source is under 16 someone must have responsibility for ensuring that an appropriate adult is present at meetings (parent, guardian, someone who has assumed responsibility for his/her welfare) or, failing that, anyone over 18 who is not employed by the investigating authority.

Where a source is under 18 no authorisation can be granted unless someone has carried out a risk assessment covering the likelihood of physical and psychological injury arising from the covert activities and is satisfied that the risks:

- are justified
- have been properly explained
- are understood by the source.

CHIS Judicial Approval

Once the authorisation has been completed, an application must be made to a single Magistrate under s.32A of the 2000 Act. To bring the directed surveillance authorisation into force, the Magistrate must be satisfied:

(a) That at the time of the grant there were reasonable grounds for believing that the requirements of section 29(2) (e.g. necessary, proportionate, plus handler, controller and record keeping in place) and any requirements imposed by section 29(7)(b) (juveniles requirements) were satisfied in relation to the authorisation; and

(b) The relevant conditions were satisfied in relation to the authorisation (i.e. section 2A(6) properly designated); and

(c) At the time when the relevant judicial authority is considering the matter, there remain reasonable grounds for believing that the requirements of section 29(2) and any requirements imposed by virtue of section 29(7)(b) are satisfied in relation to the authorisation.

The model forms for renewal and cancellation of authorisations are attached to this document at Appendices C, D and E.

TRAINING

Training is provided on a regular basis for authorising officers and staff who may be involved in RIPA investigations.

Training was held in November 2012 on the new procedures and a further session was held in March 2013 for officers unable to attend in November.

Oversight by the Office of the Surveillance Commissioners

Oversight of the process is carried out by the Office of the Surveillance Commissioners by way of an inspection every couple of years by an Assistant Surveillance Commissioner (a High Court Judge). Such inspections include interviews with key personnel, examination of RIPA applications, authorisations, the central record, policy documents and an evaluation of processes and procedures. Inspection reports are restricted and only seen by the local authorities concerned.

FURTHER GUIDANCE

Relevant legislation:

The Human Rights Act 1998
The European Convention for the Protection of Human Rights and Fundamental Freedoms
Regulation of Investigatory Powers Act 2000

Codes of Practice:

Home Office – www.homeoffice.gov.uk
Office of Surveillance Commissioners