Rutland County Council

REGULATION OF INVESTIGATORY POWERS ACT 2000 (RIPA)

FOR THE USE OF COVERT SURVEILLANCE, COVERT HUMAN INTELLIGENCE SOURCES ("CHIS") and THE ACQUISITION AND DISCLOSURE OF COMMUNICATIONS DATA

Version & Policy Number	**Version 1**
Guardian	**Head Of Corporate Governance**
Date Produced	**November 2014**
Next Review Date	**November 2017**

Approved by Cabinet	**December 2014**

CONTENTS

BACKGROUND

The Human Rights Act 1998 (which became effective on the 2nd October 2000) incorporates into UK law the European Convention on Human Rights, the effect of which is to protect an individual's rights from unnecessary interference by the "State".

The relevant parts of the Regulation of Investigatory Powers Act 2000 (*RIPA*) are Part II which came into force on 25th September 2000 and regulates covert investigations and Part 1 Chapter II, the acquisition and disclosure of communications data which came into force on 5th January 2004. Further provisions came into effect through the Protection of Freedoms Act 2012. Chapter 2 of this Act amends RIPA 2000 in that it introduces the necessity for judicial approval for local authorities engaging RIPA. These provide a framework within which the "State" (the specified public bodies) can work to ensure that law enforcement and other important functions can effectively protect society as a whole.

The Public Bodies defined in *RIPA* include Local Authorities and, therefore, Rutland County Council District Council's activities are subject to the *RIPA* framework.

The purpose of this guidance is to:

- explain the scope of *RIPA* and the circumstances where it applies
- provide guidance on the authorisation procedures to be followed .

The Council has had regard to the Codes of Practice produced by the Home Office in preparing this guidance. These can be accessed via the following link:

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

1. RIPA - PART II COVERT SURVEILLANCE

INTRODUCTION

1.1 There are a number of investigation activities that are covered by *RIPA*. These are known as: Directed Surveillance; Intrusive Surveillance and the use of a Covert Human Intelligence Source (CHIS). These are explained later in this document and the flowcharts in the Appendix provide a straightforward approach to determining whether *RIPA* applies and, if so, which provisions apply.

The Chief Executive, Directors and Head of Corporate Governance are responsible for authorising applications for directed surveillance or the use of a CHIS. References to the "Authorising Officer" should be read as

referring to any of the above; applications for approval under *RIPA* should be submitted to an Authorising Officer for consideration.

RIPA specifies that directed surveillance or the use of a CHIS by Councils can only be undertaken for the following reason:

"for the purpose of preventing or detecting crime or of preventing disorder;"

Authorisation under *RIPA* gives lawful authority to carry out directed surveillance and to use a CHIS. Before approving applications, the Authorising Officer must have regard to the necessity and proportionality of the application. Proportionality means that the action taken must be appropriate, fair and sufficient and that a sledgehammer should not be used to crack a nut. In order for the Authorising Officer to be satisfied that proportionality has been addressed, the following elements 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 le alternatives, of obtaining the necessary result;
- evidencing, as far as reasonably practicable, what other methods had been considered and why they were not implemented.

For example, if the evidence can be gained without surveillance then there should be no authorisation or, if sufficient evidence can be gained in one surveillance/visit then four must not be taken. But, once obtained, the authorisation helps to protect the Council and its officers from complaints of interference with the rights protected by Article 8 of the European Convention on Human Rights (the right to private and family life).

It should be noted that the Council **does not, *under any circumstances,*** have the power to undertake what is defined as "Intrusive Surveillance".

Staff should refer to the Home Office Codes of Conduct for supplementary guidance.

The Codes do not have the force of statute, but are admissible in evidence in any criminal and civil proceedings. As stated in the codes,

"If any provision of the code appears relevant to a question before any Court or tribunal considering any such proceedings, or to the tribunal established under *RIPA*, or to one of the commissioners responsible for overseeing the powers conferred by *RIPA*, it must be taken into account".

Deciding when authorisation is required involves making a judgement. Section 1.3 of this guidance gives some examples and Section 1.4 explains the authorisation process. If you are unclear about any aspect of the process, seek the advice of the Authorising Officer. If they are unable to answer your questions they must seek advice from the Head of Corporate Governance and/or the Council's Legal Services Team.

However, **IF YOU ARE IN ANY DOUBT** about whether a course of action requires an authorisation, **REFER IT FOR AUTHORISATION.** (If you are unable to secure an authorisation it is likely that your application does not comply with the law).

Teams of the Council that undertake surveillance that is covered by *RIPA* may wish to develop specific guidance on the applicability of RIPA to their particular circumstances. Such an approach is to be encouraged but the relevant Team Manager must ensure that any "local" guidance does not conflict with this corporate document.

1.2 DEFINITIONS

What is meant by:

Surveillance?

Surveillance includes:

a) monitoring, observing or listening to persons, their movements, their conversations or their other activities or communication and, for the purposes of *RIPA*, the term persons includes "any organisation and any association or combination of persons", this will include limited companies, partnerships, co-operatives etc;

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

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

Covert Surveillance?

Covert surveillance is that carried out in a manner calculated to ensure that persons subject to surveillance are unaware it is or may be taking place.

If activities are open and not hidden from the persons subject to surveillance, the *RIPA* framework does not apply.

Directed surveillance?

Surveillance is 'Directed' for the purposes of *RIPA* if it is covert, but not intrusive and is undertaken :

a) for the purposes of a specific investigation or a specific operation: and

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

c) 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 the carrying out of the surveillance.

Intrusive surveillance?

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; or

c) is carried out by means of a surveillance device in relation to anything taking place on any residential premises or in any private vehicle but is carried out without that device being present on the premises or in the vehicle, where the device is such that it consistently provides information of the same quality and detail as might be expected to be obtained from a device actually present on the premises or in the vehicle.

Covert Human Intelligence Source (CHIS)

A person is a Covert Human Intelligence Source if:

a) the source establishes or maintains a personal or other relationship with a person for the covert purpose of facilitating the doing of anything falling within paragraph b) or c) below,

b) the source covertly uses such a relationship to obtain information or provide access to any information to another person; or

c) the source covertly discloses information obtained by the use of such a relationship or as a consequence of the existence of such a relationship.

Covert Purpose?

A purpose is covert, in relation to the establishment or maintenance of a personal or other relationship, **if and only if,** the relationship is conducted in a manner that is calculated to ensure that one of the parties to the relationship is unaware of the purpose behind the relationship.

It is not the Council's policy to use a CHIS. If any officer considers that a CHIS should be used in any particular case, they should discuss the matter with the Head of Corporate Governance before seeking authorisation.

Private Information?

Private information is any information relating to a person's (see the definition in surveillance part a above) private or family life.

For example, if part of an investigation is to observe a member of staff's home to determine their comings and goings then that surveillance would, almost certainly, gather private information, as would surveillance of an individual selling counterfeit goods as the surveillance may provide information about the earnings that the person made from the sales.

Confidential Material?

a) matters subject to legal privilege;
b) confidential personal information; or
c) confidential journalistic material.

- Matters subject to legal privilege includes both oral and written communications between a professional legal adviser and his/her client (or any person representing his/her client) made in connection with the giving of legal advice to the client or in contemplation of legal proceedings and for the purposes of such proceedings, as well as items enclosed with or referred to in such communications. Communications and items held with the intention of furthering a criminal purpose are not matters subject to legal privilege (see NB1 below)

- "Confidential Personal Information" is information held in confidence concerning an individual (whether living or dead) who can be identified from it, and relating:

  a) to his/her physical or mental health; or
  b) 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 (see NB2 below). It includes both oral and written information and also communications as a result of which personal information is acquired or created. Information is held in confidence if:
  c) it is held subject to an express or implied undertaking to hold it in confidence; or
  d) it is subject to a restriction on disclosure or an obligation of secrecy contained in existing or future legislation.

- "Confidential Journalistic Material" includes material acquired or created for the purposes of journalism and held subject to an undertaking to hold it in confidence, as well as communications resulting in information being acquired for the purposes of journalism and held subject to such an undertaking.

NB 1. Legally privileged communications will lose their protection if there is evidence, for example, that the professional legal adviser is intending to hold or

use them for a criminal purpose; privilege is not lost if a professional legal adviser is advising a person who is suspected of having committed a criminal offence. The concept of legal privilege shall apply to the provision of professional legal advice by any agency or organisation.

NB 2. Confidential personal information might, for example, include consultations between a health professional or a professional counsellor and a patient or client, or information from a patient's medical records.

1.3 DOES RIPA PART II APPLY TO MY SITUATION?

Is it for the purposes of a specific investigation or a specific operation?

The test is if the surveillance is directed at a known individual or group the provisions of RIPA will cover the investigation. In respect of other situations, such as CCTV cameras that are readily visible to anyone walking around the area, their use is not governed by RIPA. However, if the cameras are used as part of an operation to observe a known individual or group it is very likely that RIPA will apply and an appropriate authorisation will be required.

Is the surveillance likely to obtain private information about a person?

If it is likely that observations will result in the obtaining of private information about any person, then RIPA may apply.

If in doubt, it is safer to seek authorisation

Is the Surveillance Intrusive?

Directed surveillance turns into intrusive surveillance if it is carried out involving anything that occurs on residential premises or any private vehicle and involves the present of someone on the premises or in the vehicle or is carried out by means of a (high quality) surveillance device.

If the device is not on the premises or in the vehicle, it is only intrusive surveillance if it consistently produces information of the same quality as if it were.

Commercial premises and vehicles are therefore excluded from intrusive surveillance.

The Council is NOT authorised to carry out intrusive surveillance.

Is the surveillance an immediate response to event or circumstances where it is not reasonably practicable to get authorisation?

The Home Office guidance indicates that this is to take account of an immediate response to something happening during the course of an observer's work, which is unforeseeable. If this occurs, the surveillance will not require prior

authorisation. It should be noted that general observation forming part of an officer's normal activities, for example, planning enforcement, will not be within the scope of *RIPA*.

However, if, as a result of an immediate response, a specific investigation subsequently takes place that investigation will be within the scope of *RIPA.*

1.4 AUTHORISATIONS, RENEWALS AND DURATION UNDER RIPA PART II

1.4.1 The conditions for authorisation

Directed Surveillance

For directed surveillance no officer shall grant an authorisation for the carrying out of directed surveillance unless he believes:

a) that an authorisation is *necessary* that is, it has to be gained to be able to gather the information needed for the detection or prevention of crime. (Also, see the relevant Codes of Practice).
b) the authorised surveillance is *proportionate* to what is sought to be achieved by carrying it out and that a sledgehammer is not being used to crack a nut. Any surveillance that is carried out must be at the most appropriate level to achieve the objectives of the investigation. (Additional guidance is available in the relevant Codes of Practice).

An authorisation under *RIPA* will only be given if the work is:

"for the purpose of preventing or detecting crime or of preventing disorder;"

The onus is on the people authorising the surveillance activity to satisfy themselves that the action to be taken is necessary and proportionate.
In order to ensure that authorising officers have sufficient information to make an informed decision it is important that detailed records are maintained. An application form must be completed.

It is also sensible to make any authorisation sufficiently wide to cover all the means required as well as being able to provide effective monitoring of what was done against the actions that had been authorised.

See the flowchart in the Appendix, page 2.

Use of Covert Human Intelligence Sources

The same principles as Directed Surveillance apply (see paragraph 1.4.1 above). However, as it is the Council's policy not to use CHIS, further guidance is not included in this document. The Head of Corporate Governance must be contacted if an officer considers that the use of a CHIS is appropriate in any particular case.

1.4.2 Provisions of RIPA PART II

For *urgent* grants or renewals, oral authorisations are acceptable, but should be followed up with a written application as soon as possible thereafter. Urgent grants are those where authorisation would be needed but the circumstances are such that if a grant was waited for then the time for the gathering of the information would have passed and the opportunity missed. In all other cases, authorisations must be in writing.

Directed surveillance and the use of a CHIS will be applied for on the relevant forms, even if they relate to the same surveillance target.

Authorisations **must** be cancelled as soon as they are no longer required, and, in any event, on or before the expiry date of the authorisation.

Authorisations only last, if not renewed:

- Any authorisation granted or renewed orally, (or by a person whose authorisation was confirmed to urgent cases) expire after 72 hours, this period beginning with the time of the last grant or renewal;

- A written authorisation to use a CHIS expires after 12 months from the date of last renewal or

- in all other cases (i.e. directed surveillance) 3 months from the date of their grant or latest renewal.

Any person entitled to grant a new authorisation, as described above, can renew an existing authorisation, on the same terms as the original authorisation, at any time before the original ceases to have effect.

A CHIS application should not be renewed unless a thorough review has been carried out and the authorising officer has considered the results of the review when deciding whether to renew or not. A review must cover what use has been made of the source, the tasks given to them and information obtained.

The benefits of obtaining an authorisation are described in section 3 below.

1.4.3 Factors to Consider

General

Any person giving an authorisation must satisfy themselves, based on the information in the application and their knowledge of the service that:

- the authorisation is <u>necessary</u>
- the surveillance <u>is proportionate</u> to what it seeks to achieve.

Particular consideration should be given to intrusion on, or interference with, the privacy of persons other than the subject(s) of the application (**known as**

collateral intrusion). 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.

An application for an authorisation **must include an assessment of the risk of any collateral intrusion or interference.** The authorising officer will take this into account, particularly when considering the proportionality of the directed surveillance or the use of a CHIS.

Those carrying out the covert directed surveillance should inform the Authorising Officer if the operation/investigation unexpectedly interferes with the privacy of individuals who are not the original subjects of the investigation or covered by the authorisation in some other way. In some cases the original authorisation may not be sufficient and consideration should be given to whether a separate authorisation is required.

Any person giving an authorisation will also need to be aware of particular sensitivities in the local community where the directed surveillance is taking place or of similar activities being undertaken by other public authorities that could impact on the deployment of surveillance.

The keeper of the central register will inform the Investigating officers of the review time. **The Investigating officer is responsible for ensuring that approvals, reviews, renewals and recommendations for cancellation are made and timely.**

The fullest consideration should be given in cases where the subject of the surveillance might reasonably expect a high degree of privacy, for instance at his/her home, or where there are special sensitivities. Care must be exercised, particularly in relation to residential premises, to avoid carrying out any surveillance that may be deemed to fall under the definition of Intrusive Surveillance (because a local authority is not empowered to undertake intrusive surveillance).

Spiritual Counselling

No operations should be undertaken in circumstances where investigators believe that surveillance will lead to them intrude on spiritual counselling between a Minister and a member of his/her faith. In this respect, spiritual counselling is defined as conversations with a Minister of Religion acting in his/her official capacity where the person being counselled is seeking or the Minister is imparting forgiveness, or absolution of conscience.

Confidential Material

RIPA does not provide any special protection for confidential material (see the definition in the Appendix). Nevertheless, such material is particularly sensitive, and is subject to additional safeguard under this code. In cases where the likely consequence of the conduct of a source would be for any person to acquire

knowledge of confidential material, the deployment of the source should be subject to special authorisation by the Chief Executive.

In general, any application for an authorisation that is likely to result in the acquisition of confidential material should include an assessment of how likely it is that confidential material will be acquired. Special care should be taken where the target of the investigation is likely to be involved in handling confidential material. Such applications should only be considered in exceptional and compelling circumstances with full regard to the proportionality issues this raises.

The following general principles apply to confidential material acquired under authorisations:

- Those handling material from such operations should be alert to anything that may fall within the definition of confidential material. Where there is doubt as to whether the material is confidential, advice should be sought from the Head of Corporate Governance before further dissemination takes place;

- Confidential material should be disseminated only where an appropriate officer (having sought advice from the Head of Corporate Governance) is satisfied that it is necessary for a specific purpose

- The retention or dissemination of such information should be accompanied by a clear warning of its confidential nature. It should be safeguarded by taking reasonable steps to ensure that there is no possibility of it becoming available, or its content being known, to any person whose possession of it might prejudice any criminal or civil proceedings related to the information. Any material of this nature will be reviewed on a monthly basis by the Team Manager.

- Confidential material should be destroyed as soon as it is no longer necessary to retain it for a specified purpose.

Combined authorisations

A single authorisation may combine two or more different authorisations under RIPA (but cannot include an authorisation for intrusive surveillance activity).

In cases of joint working with other agencies on the same operation, the lead agency should be responsible for authorisations. Council officers should ensure that there is agreement between the agencies at the start of the operation as to which will be the lead agency for this purpose.

Handling and disclosure of the products of surveillance

Authorising Officers are reminded of the guidance relating to the retention and destruction of confidential material as described above.

The Authorising Officer should retain RIPA related documents for a period of three years. However, where it is believed that the records could be relevant to

pending or future criminal proceedings, they should be retained for a suitable further period, commensurate to any subsequent review.

Authorising officers must ensure compliance with the appropriate data protection requirements and the relevant codes of practice in the handling and storage of material. Where material obtained by surveillance is wholly unrelated to a criminal or other investigation, or to any person who is the subject of the investigation, and there is no reason to believe it will be relevant to future civil or criminal proceedings, it should be destroyed immediately. Consideration of whether or not unrelated material should be destroyed is the responsibility of the Authorising Officer.

Material obtained through the proper use of the RIPA authorisation procedures can be used for relevant Council purposes. However, the transfer of such information outside the Council, other than in pursuance of the grounds on which it was obtained, should be authorised only in the most exceptional circumstances and should always only occur following consideration of the appropriate Data Protection legislation.

The Use of Covert Human Intelligence Sources (CHIS)

It is not the Council's policy to seek, cultivate or develop a relationship with a potential external or professional source. If the use of a CHIS was to be considered in exceptional circumstances, a risk assessment of the safety and welfare of any employee potentially involved would be an essential pre-requisite of an authorisation.

Register of Authorisations

The Head of Corporate Governance is responsible for maintaining a central register of authorisations. The register will record the date of the authorisation, the name of the authorising officer and the location of the file where the authorised application will be retained. The Officer who has authorised the application must contact the Head of Corporate Governance to provide the specified information and to obtain a reference number for the authorisation. This must be done on the day that the application is authorised. The Authorising Officer must then ensure that the authorised application is filed in the location notified to the Head of Corporate Governance. The original will be kept in the Central register. A Director who is permitted to authorise applications under *RIPA* will ensure that their Team maintains appropriate files for all applications, approvals and cancellations. Cancellations must be attached to the relevant authorised applications.

2. RIPA PART I CHAPTER II – THE ACQUISITION AND DISCLOSURE OF COMMUNICATIONS DATA

2.1 INTRODUCTION

Part I Chapter II (sections 21 – 25 of RIPA) came into force on 5th January 2004. It regulates the acquisition and disclosure of communications data. It provides powers for the Council to gain communications information when carrying out investigations. It also regulates information previously gained without regulations, which now has to be authorised.

The process is similar to that of the authorisation of directed surveillance and CHIS, but has extra provisions and processes.

The purpose of the introduction is the same, that is, to protect people's human rights. The effect of not gaining authorisation when needed is the same. The Council leaves itself open to a challenge under the Human Rights Act 1998 and the evidence gained without authorisation may not be admissible in court.

RIPA specifies that the only purpose for which the Council can gather communication data is in the:

'Prevention and detection of crime or preventing disorder'

Staff should refer to the Home Office Codes of Conduct for supplementary guidance

The Codes do not have the force of statute but are admissible in evidence in any criminal and civil proceedings.

2.2 WHAT IS COMMUNICATIONS DATA?

The definition of communications data includes information relating to the use of a communications service but it does not include the contents of the communication itself. It is broadly split into three categories:

- Traffic data – where a communication was made from, to who and when
- Service data – the use made of a service by any person e.g. itemised telephone records
- Subscriber data – any other information held or obtained by an operator on a person they provided a service to.

This Council is restricted to subscriber and service use data and even then only for the purpose of preventing or detecting crime and disorder. For example a benefit fraud investigator may be able to get access to an alleged fraudster's mobile phone bills.

The word ‘data’ in relation to a postal item means anything written on the outside such as an address. Officers at the Council have previously been able to apply for the new address of a person that they were investigating, that is the re direction details. A request form was completed and the post office supplied the information. This activity is now regulated and authorisation needs to be gained.

THE CODE DOES NOT COVER THE INTERCEPTION OF COMMUNICATIONS (IE THE CONTENTS OF ANY COMMUNICATIONS INCLUDING THE CONTENT OF AN E-MAIL, OR INTERACTION WITH WEB SITES)

2.3 AUTHORISATIONS, NOTICES, RENEWALS AND DURATION

2.3.1 AUTHORISATIONS AND NOTICES

The Code states that a ‘designated person’, must decide whether authorisation is necessary and proportionate to the action to be taken. The designated person is in effect the Authorising Officer. The designated persons at this Council are the Chief Executive and Directors.

There are two ways to authorise access to communications data.

(a) Authorisation under 22(3). This allows the authority to collect the data itself. This may be appropriate where:

- The postal or telecommunications operator is not capable of collecting or retrieving the communications data;
- It is believed that the investigation may be prejudiced if the postal or telecommunications operator is asked to collect the data itself;
- There is a prior agreement in place between the relevant public authority and the postal or telecommunications operator as to the appropriate mechanisms for the disclosure of data.

(b) By a notice under section 22(4). A notice is given to a postal or telecommunications operator and requires that operator to collect or retrieve the data and provide it to the authority.
The designated person decides whether or not an authorisation should be granted.

The designated person must take account of the following points when deciding whether to authorise the application or not.

- Is the accessing of data for the prevention or detection of crime or disorder?
- Why is obtaining the data necessary for that purpose?
- Is obtaining access to the data by the conduct authorised proportionate to what is being sort to be achieved? That is what conduct are you authorising and is it proportionate?
- Is the accessing of the data likely to result in collateral intrusion? If so, is the access still justified?

- Is any urgent time scale justified?

  The designated person will make a decision whether to grant the authorisation based upon the application made. The application form should subsequently record whether or not the application was approved or not, by whom and the date. A copy of the application must be kept by the officer until it has been inspected by the Commissioner.

  If the application is authorised and the notice needs to be served, then only the notice is served upon the postal or telecommunications officer.

  The application form and the authorisation itself are not served upon the holder of the communications data. The authorisation and notice are in the standard form and are available on the Shared drive.

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

2.3.2 PROVISIONS OF RIPA

Single Point of Contact (SPOC)

Notices and authorisations for communications data should be channelled through a SPOC. The Code states that this is to provide an effective system in that the SPOC will deal with the postal or telecommunications operator on a regular basis. The SPOC will advise the Authorising Officer/designated person on whether an authorisation and/ or notice is appropriate.

The SPOC should be in a position to:

- Where appropriate, assess whether access to communications data is reasonably practical for the postal or telecommunications operator;
- Advise applicants and designated persons on the practicalities of accessing different types of communications data from different postal or telecommunications operators;
- Advise applicants and designated persons on whether communications data falls under section 21(4)(a), (b) or (c) of the Act, that is traffic, service or subscriber data;
- Provide safeguards for authentication;
- Assess any cost and resource implications to both the public authority and the telecommunications operator.

The SPOC at this Council is the Head of Corporate Governance, who is formally accredited through the Home Office.

Oral Authority

An oral application and approval can only be made on an urgent basis for the purpose set out in section 22(2)(g) of the Act. That is

> "for the purpose, in emergency, of preventing death or injury or any damage to a person's physical or mental health, or of mitigating any injury or damage to a person's physical or mental health".

That is not a purpose under which the council is able to collect communications data and therefore oral authorisations are not possible.

Duration

Authorisations and notices will only be valid for one month beginning from the date when it was granted. If the information can be collected in a shorter time period then that should be specified. This would accord with the proportionality element of the decision making.

The postal or telecommunications operator need only comply with the request if it is reasonably practicable to do so.

Renewal

An authorisation or notice can be renewed at any point during the month that it is valid by following the same procedure as in obtaining a fresh authorisation.

Cancellations

The duty to cancel falls on the designated person who authorised it. The notice shall be cancelled as soon as it is no longer necessary or is no longer proportionate to what is being sort to be achieved.

Authorisations should also be cancelled. In the case of a section 22(4) notice, the postal or communications operator shall be informed of the cancellation.

Retention

Applications, authorisations and notices will be retained by the authority until they have been audited by the Commissioner. The authority should also keep a record of the dates that the notices and authorisations were started and cancelled. A copy of each form should be kept by the investigating Team and the originals kept in the Central Register. It shall be the responsibility of the designated person to ensure that the records are accurate and kept up to date.

Combined Authorisations

Applications for communications data may only be made by persons in the same authority as a designated person. There cannot, therefore, be any combined authorisations.

Errors

Where any errors have occurred in the granting of authorisations or the giving of notices, a record should be kept and a report and explanation sent to the Commissioner as soon as practical.

3. BENEFITS OF OBTAINING AUTHORISATIONS UNDER RIPA

Authorisation of surveillance, human intelligence sources and the acquisition and disclosure of communications data.

RIPA states that:

"If authorisation confers entitlement to engage in a certain conduct and the conduct is in accordance with the authorisation, then it shall be "lawful for all purposes".

However, the opposite is not true – i.e. if you do not obtain *RIPA* authorisation it does not make any conduct unlawful (e.g. use of intrusive surveillance by local authorities). It just means you cannot take advantage of any of the special RIPA benefits and you may have to justify infringing a person's Human Rights and any evidence you place before the courts may be subject to challenge in respect of the processes used to obtain the evidence (s78 Police and Criminal Evidence Act 1984).

RIPA states that a person shall not be subject to any civil liability in relation to any conduct of his which –

a) is incidental to any conduct that is lawful by virtue of an authorisation; and

b) is not itself conduct for which an authorisation is capable of being granted under a relevant enactment and might reasonably be expected to have been sought in the case in question.

However, **IF YOU ARE IN ANY DOUBT** about whether a course of action requires an authorisation, **REFER IT FOR AUTHORISATION**. (If you are unable to secure an authorisation it is likely that your application does not comply with the law).

4. SCRUTINY AND TRIBUNAL

As of 1 November 2012 the Council has to obtain an order from a Justice of the Peace approving the grant or renewal of any authorisation for the use of directed surveillance or CHIS before the authorisation can take effect and the activity be carried out. The Council can only challenge a decision of the Justice of the Peace on a point of law by way of judicial review.

Consideration must be given to 'Crime Threshold' which means that a Local Authority can now only grant an authorisation under RIPA for the use of directed

surveillance where the Local Authority is investigating particular types of criminal offences. These are criminal offences which attract a maximum custodial sentence of six months or more or relate to the underage sale of alcohol or tobacco.

The Chief Executive shall be the Senior Responsible Officer who will:

- ensure compliance with the Council's policy, relevant RIPA legislation and guidance;
- engage with Commissioners and inspectors when the Council's inspection is due (usually every three years);
- oversee any post-inspection action plans recommended or approved by a Commissioner.

This policy shall be reviewed, and where necessary amended, at least once a year. If requiring amendment, the revised policy shall be presented to and considered by the following:

- the Strategic Management Team
- the Audit and Risk Committee

The Senior Responsible Officer (or delegated representative) will report to the relevant Council committee, detailing the Council's use of RIPA powers, annually. The Council's elected members will not be involved in any decisions made on specific authorisations granted.

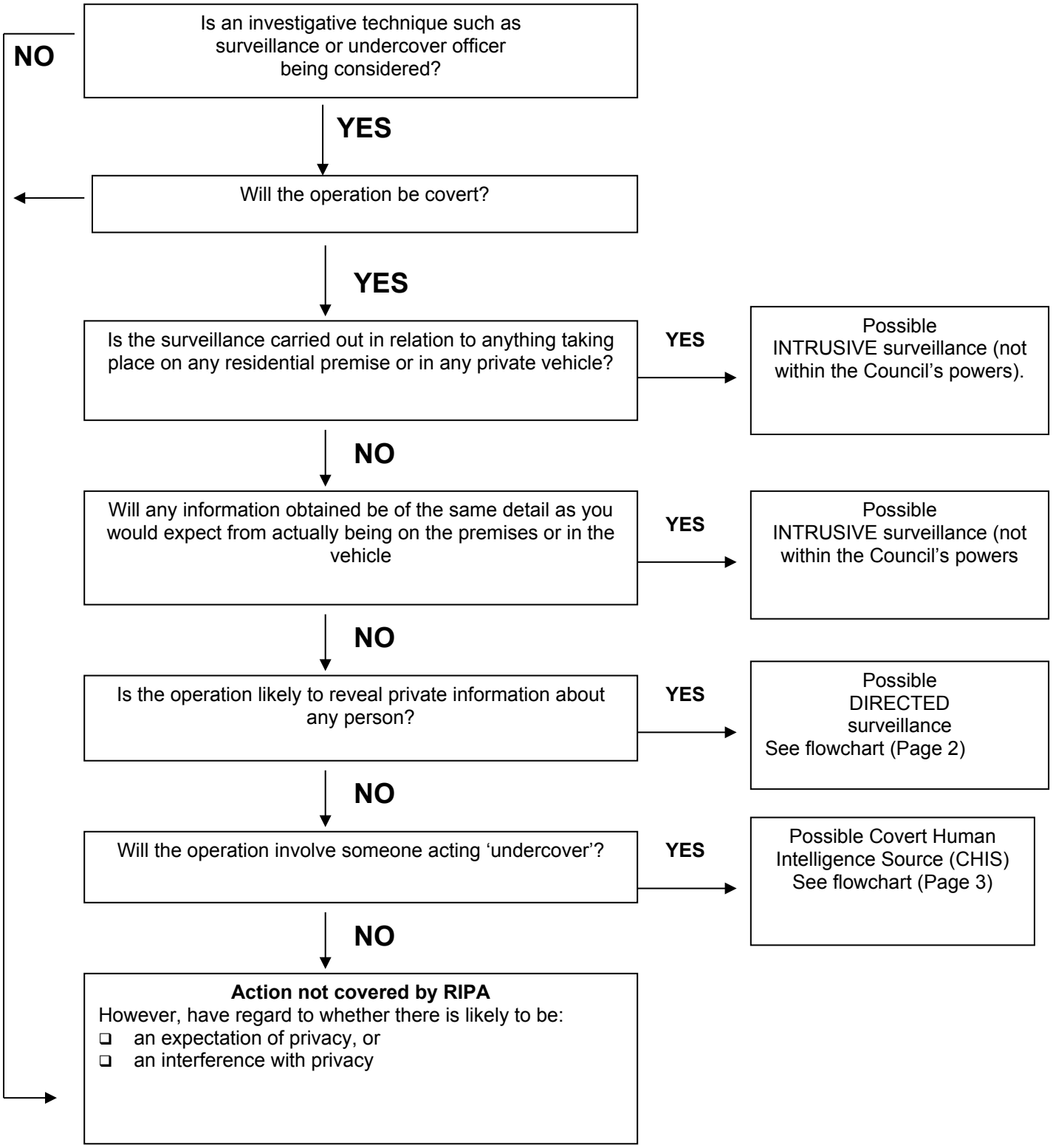
RIPA set up the Office of the Surveillance Commissioner to regulate the conduct of public bodies and to monitor their compliance with *RIPA*. The Chief Surveillance Commissioner will keep under review, among other things, the exercise and performance of duties, imposed in *RIPA* by the persons on whom those duties are conferred or imposed. This includes authorising directed surveillance and the use of covert human intelligence sources.

A tribunal has been established to consider and determine complaints made under *RIPA* if it is the appropriate forum. Persons aggrieved by conduct, e.g. directed surveillance, can make complaints. The forum hears application on a judicial review basis. Claims should be brought within one year unless it is just and equitable to extend that period.

The tribunal can order, among other things, the quashing or cancellation of any warrant or authorisation and can order destruction of any records or information obtained by using a warrant or authorisation, and records of information held by any public authority in relation to any person. The Council is, however, under a duty to disclose or provide to the tribunal all documents they require if:

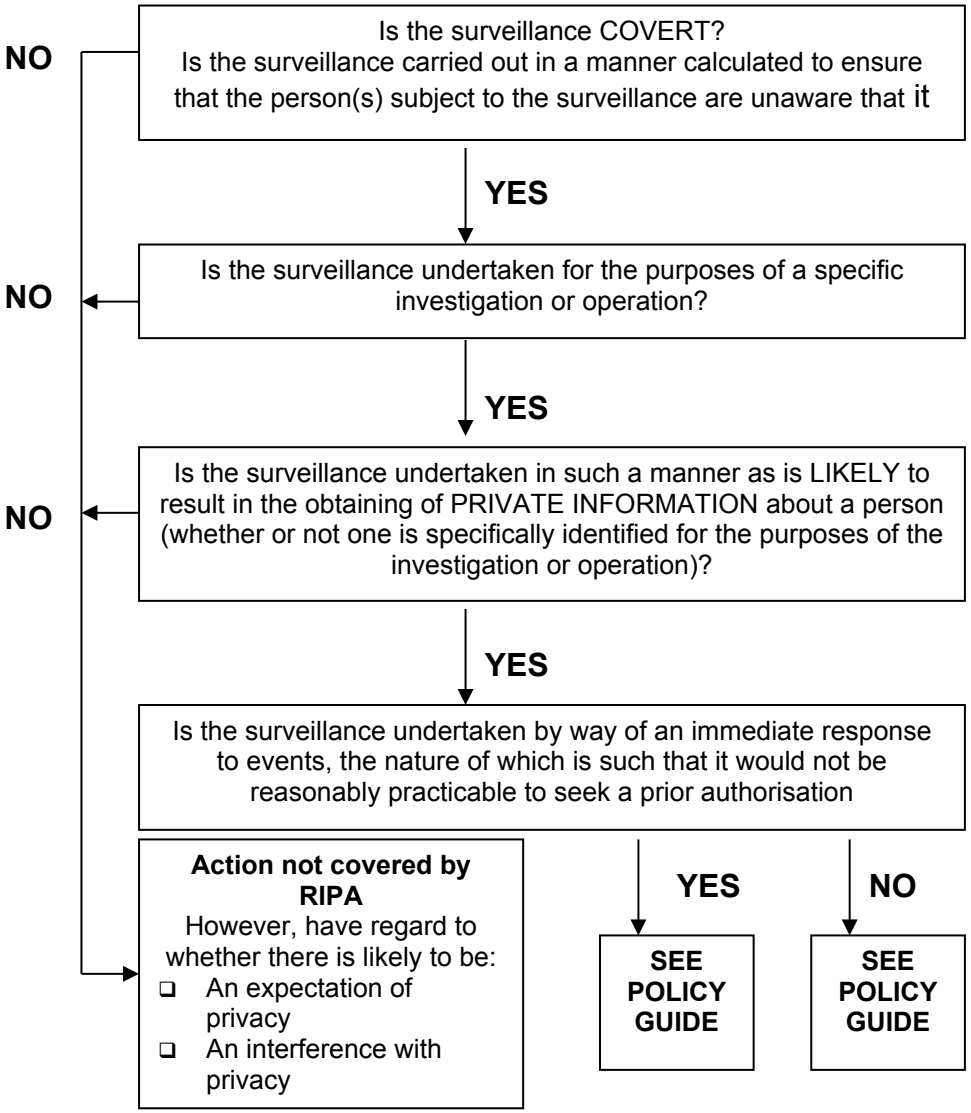
- A Council officer has granted any authorisation under RIPA.
- Council employees have engaged in any conduct as a result of such authorisation.
- A disclosure notice requirement is given.

SURVEILLANCE SUMMARY



PROCESS FLOWCHARTS

DIRECTED SURVEILLANCE



INTERPRETATION

COVERT see section 26(9) RIPA

SURVEILLANCE see Section 48(2) to 48(4) RIPA includes monitoring, observing or listening to persons, their movements, their conversations or their activities or communications.

DIRECTED SURVEILLANCE see Section 26(2) RIPA

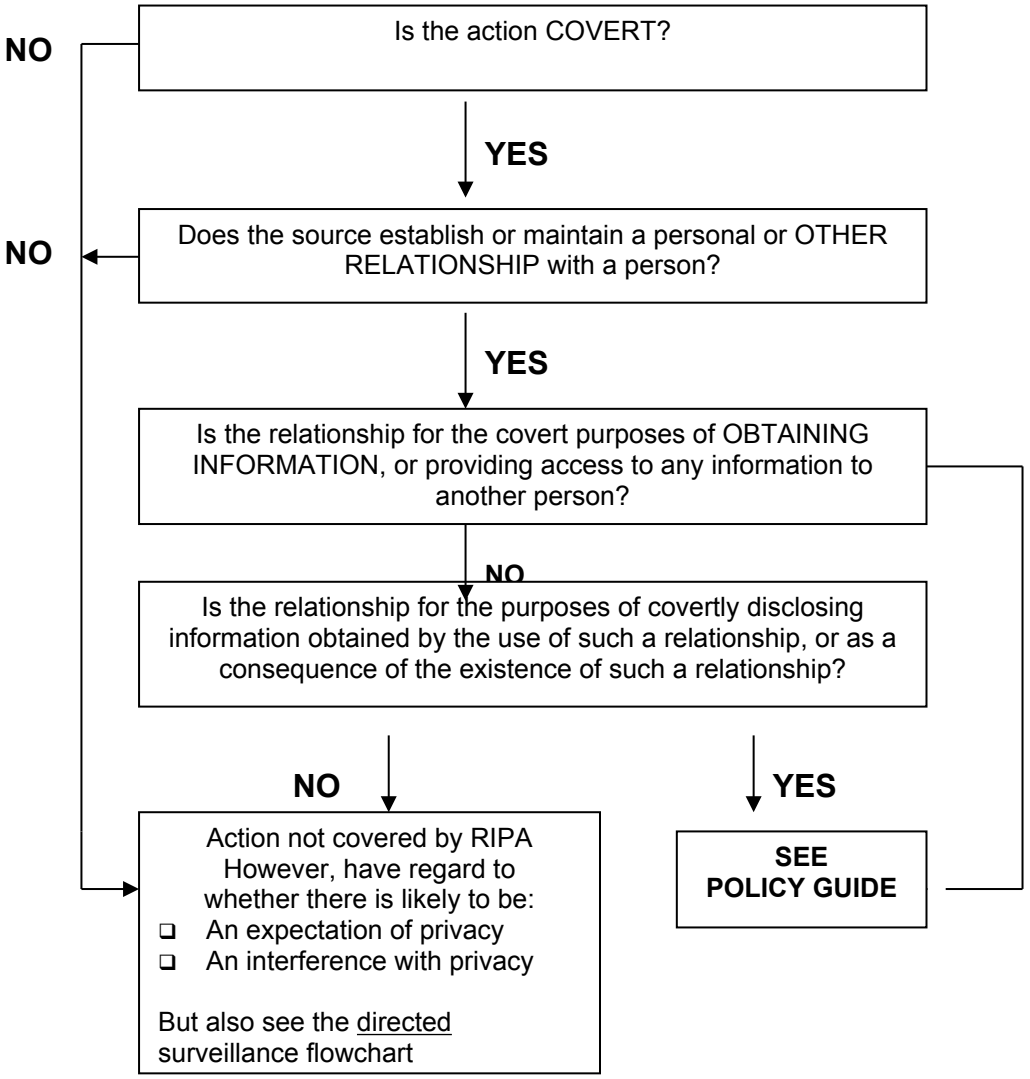
PERSON see Section 81(1) RIPA. Includes any organisation and any association or combination of persons

PRIVATE INFORMATION see Section 26(10) RIPA in relation to a person, includes any information relating to his private or family life.
'Private Information' should be given a wide interpretation and should not be restricted to what might be considered to be 'secret' or 'personal' information. Information that is in the open for all to see (for example: who is visiting a premise) may be deemed to be private information.

CONFIDENTIAL MATERIAL see paragraph 3 of the Code of Practice confidential information includes matters subject to legal privilege, confidential journalistic material and confidential personal information, for example medical records or religious material.

For further interpretation see Sections 48 & 81 RIPA, including Explanatory Notes to RIPA & Codes of Practice on Covert Surveillance & Use of a CHIS

COVERT HUMAN INTELLIGENCE SOURCE



INTERPRETATION

COVERT see section 26(9) RIPA

COVERT PURPOSES. see Section 26(9)(b)&(c) RIPA

CHIS See Section 26(8) RIPA. The use of a CHIS is NOT surveillance. (see Section 48(3) RIPA)

PERSONAL OR OTHER RELATIONSHIP This is not defined, but a wide interpretation should be applied.

INFORMATION This is not defined but section talks about information in general and is not restricted to private information as is the case with directed surveillance

CONFIDENTIAL MATERIAL see paragraph 3 of the Code of Practice confidential information includes matters subject to legal privilege, confidential journalistic material and confidential personal information, for example medical records or religious material.

For further interpretation see Sections 48 & 81 RIPA, including Explanatory Notes to RIPA & Codes of Practice on Covert Surveillance & Use of a CHIS.

A large print version of this document is available on request

Rutland
County Council

Rutland County Council
Catmose, Oakham, Rutland LE15 6HP

01572 722 577
enquiries@rutland.gov.uk
www.rutland.gov.uk