APPENDIX B

Regulation of Investigatory Powers Act 2000 Policy

Date: October 2020

CONTENTS

BLABY DISTRICT COUNCIL

POLICY ON REGULATION OF INVESTIGATORY POWERS ACT 2000 (RIPA)

1. Introduction

Blaby District Council will only carry out covert surveillance where such action is justified and aims to keep such surveillance to a minimum. The policy has been produced to provide full and proper guidance for officers on:

the scope of RIPA
the circumstances where it applies; and
the authorisations procedures to be followed

This policy document supports the third corporate aim of reducing the fear of crime and anti social behaviour by ensuring the Council has the appropriate tools and processes in place to allow use of this power where needed and justified.

2. The Scope of the Act

The Regulation of Investigatory Powers Act 2000 ("the Act") regulates the use of investigatory powers of various bodies including local authorities so that they do not breach human rights.

The Act is supplemented by:

- Home Office guidance (October 2012) Appendix D
- The Covert Surveillance and Property Interference Statutory Code of Practice Appendix A
- The Covert Human Intelligence Sources ("CHIS") Statutory Code of Practice Appendix B
- The Office of Surveillance Commissioners Procedures and Guidance Appendix C

Where the directed covert surveillance of an individual or group of individuals, or the use of a CHIS is necessary the Act:

- Requires prior authorisation of directed surveillance
- Prohibits the Council from carrying out intrusive surveillance
- Requires authorisation of the conduct and use of a CHIS
- Requires safeguards for the conduct and use of CHIS
- Permits the Council to acquire communications data in certain circumstances

The Act does not affect other powers the Council has to obtain information using other methods, for example, it does not affect the District Council's current powers to obtain information via the DVLA or to get information from the Land Registry as to the ownership of a property.

CCTV

The use of CCTV is not covert where we make members aware it is being used by putting up signs.

You will need to obtain RIPA authorisation where:

- You intend to use existing CCTV covertly and it is pre-planned for a specific investigation or to target individuals
- If you intend to use a camera for a specific purpose, which involves prolonged surveillance on a particular person. Always be aware that though the subject might not be an individual it can include surveillance of a person, for example if you are monitoring a business it may reveal information about the private life of the owners or others.

3. Benefits of RIPA authorisations

If the Act is followed correctly any authorised action will be lawful and not breach a person's right to respect for their private and family life, home and correspondence.

Any material obtained through properly authorised covert surveillance is then admissible evidence in criminal proceedings and will not be excluded unless is found to have an adverse effect on the fairness of proceedings.

4. Scrutiny and Tribunal

4.1 External Scrutiny

The Investigatory Powers Commissioners Office (IPCO) has a duty to keep under review the exercise and performance by the relevant persons of the powers and duties under Part II of the Act, and will from time to time inspect the Council's records and procedures.

There is also a Tribunal to hear complaints from persons aggrieved by conduct on a judicial review basis.

4.2 Internal Scrutiny

The SRO and Co-ordinating Officer will review the authority's use of the Act and the Policy and Guidance document at least once a year, or when required in line with any legislative changes.

The Scrutiny Commission will review the authority's use of the Act and the Policy and Guidance document at least once a year. They will also consider internal reports on the use of the Act on a quarterly basis (if any authorisations have been granted) to ensure that it is being used consistently with this Policy and that the Policy is fit for purpose. The Members will not, however, be involved in making decisions on specific authorisations.

An elected member will not be given the details of specific operations and, specifically, will not be given the identity of CHIS nor have access to the information gained, or the detail of any surveillance.

4. Authorising Officers

The Chief Executive or Strategic Directors will consider all applications for authorisation in accordance with RIPA ("Authorising Officers"). Authorising Officers, on behalf of the Council, shall in particular ensure that: -

- there is a satisfactory reason for carrying out the surveillance
- the covert nature and extent of the investigation is necessary and proportionate to the information being sought
- proper consideration has been given to collateral intrusion
- provide guidance and training for officers and members where appropriate
- records of all authorisations are sent to the RIPA Co-ordinating Officer for entry on the Central Register.
- their relevant members of staff are suitably trained as 'Applicants' so as to avoid errors in the operation of the process and completion of relevant forms. It is important that relevant Directors, Group Managers, Service Managers and Authorising Officers take personal responsibility for the efficient and effective operation of this Policy and Guidance document within their respective areas.
- that staff who report to them follow this Policy and Guidance document and do not undertake or carry out any form of surveillance without first obtaining the relevant authorisations in compliance with this document.
- when sending copies of any forms to the RIPA Co-ordinating Officer, that they are sent in sealed envelopes marked 'RIPA – Private and Confidential'.
- relevant members of staff are aware of the Act's requirements.

5. Senior Responsible Officer

The **Strategic Director** is the SRO for the Council and is responsible for:

- The integrity of the process in place within the Council to authorise directed surveillance and CHIS
- Compliance with Part II of the Act and with the accompanying Codes of Practice
- Engagement with the IPCO when they conduct their inspections; and

- Where necessary oversee the implementation of any post-inspection action plans recommended or approved by the IPCO

6. RIPA Co-ordinating Officer / Training

The RIPA Co-ordinating Officer is the Council's Democratic Services, Scrutiny and Governance Manager. The RIPA Co-ordinating Officer is responsible for the maintenance of the Central Record of Authorisations and the collation of RIPA applications/authorisations, reviews, renewals, and cancellations. In addition, there is responsibility for providing oversight of the RIPA process within the Council and for RIPA training.

All forms should be passed through this person on the point of application to the Authorising Officer to ensure that there is a complete record of all authorisations, that the forms are correctly filled and so that statistics can be passed to the IPCO.

The SRO in conjunction with the RIPA Co-ordinating Officer shall ensure that refresher training is offered once a year to relevant officers of the Council and also give advice and training on request.

7. Definitions

'Covert' means surveillance carried out in such a manner with the intention that the person subject to it is unaware that it is or may be taking place. (s.26 (9)(a) of the Act)

'Covert human intelligence source' (CHIS) means a person who establishes or maintains a relationship with a person for the covert process of obtaining information about that person. (s.26 (8) of the Act)

'Collateral intrusion' means the intrusion on, or interference with, the privacy of persons other than the subject of the investigation.

'Directed surveillance' is defined as covert but not intrusive and undertaken:

- for a specific investigation or operations
- in such a way that is likely to result in the obtaining of private information about any person
- other than by way of an immediate response (s.26 (2) of the Act)

'Private information' includes information relating to a person's private or family life and can embrace aspects of business and professional life.

'Intrusive' surveillance is covert surveillance that is carried out in relation to anything taking place on any residential premises or in any private vehicle and involves the presence of an individual on the premises or in the vehicle or using a surveillance device. **Blaby District Council may not authorise such surveillance, it may only be carried out by the police**.

GUIDANCE - PART I

THE USE OF DIRECTED SURVEILLANCE AND COVERT HUMAN INTELLIGENCE SOURCE

1. Covert Human Intelligence Source ("CHIS")

A CHIS is any person who establishes or maintains a personal or other relationship with a person for the covert purpose or facilitation of:

(a) using that relationship to obtain information or provide access to any information to another person; or

(b) disclosure of information obtained through that relationship or as a consequence of it

It also covers where the Council ask or assist a person to be a CHIS. Officers should be aware that where someone is contacting you routinely to provide you with information you have not requested they may also be considered to be a CHIS. It is that he or she has obtained the information not by mere observation, but in the course of, or result of, the existence of, a personal or other relationship. Officers must therefore seek advice must and potentially authorisation.

Officers should be aware that befriending someone on social media for the purposes of conducing an investigation would also be a CHIS and therefore advice must be sought to seek authorisation before any action is taken.

There are additional rules regarding the use of juveniles and vulnerable individuals as CHIS's and the Democratic Services and Governance Manager must be approached for legal advice.

2. Surveillance

'Surveillance' can be:

Overt - 'non' secretive surveillance where people are aware of it.

Covert secretive surveillance where the person being watched in unaware. There are two types covered under the act, - directed surveillance and Intrusive surveillance. The Council cannot use intrusive surveillance.

Surveillance can include:

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

2.1 Overt Surveillance

Most of the surveillance carried out by the Council will be done overtly particularly where officers are behaving in the same way as a normal member of the public and/or are going about Council business openly.

It will also be overt if we inform people it will be happen, for example:

- where a noisemaker is warned (preferably in writing) that noise will be recorded if the noise continues;
- where an entertainment licence is issued subject to conditions, and the licensee is told that officers may visit without notice or identifying themselves to the owner/proprietor to check that the conditions are being met.)
- CCTV is erected due to fly tipping and signs are put up to make people aware the area is being monitored.

2.2 Directed Covert Surveillance

Directed Surveillance is surveillance which: -

- is covert; and

- is not intrusive surveillance (for definition see section 7, page 6);

- it is undertaken for the purpose of a **specific investigation** or operation in a manner **likely to obtain private information** about an individual (whether or not that person is specifically targeted for purposes of an investigation), *(Section 26(10) of the Act).*

- is not carried out in an immediate response to events where seeking authorisation under the Act unreasonable, e.g. spotting something suspicious and continuing to observe it; and

It includes the activity of monitoring, observing, listening and recording by or with the assistance of surveillance equipment.

A search for an identified person in a public place **will not** amount to directed surveillance, unless it includes covert activity that may mean you collect private information about that person or any other person. Any processing of data (e.g. taking a photograph to put on record) is an invasion of privacy.

The fact that covert surveillance occurs in a public place or on business premises does not mean that it cannot result in the obtaining of private information about a person. Prolonged surveillance targeted on a single person will undoubtedly result in the obtaining of private information about their and others that s/he comes into contact, or associates, with.

'Authorising Officers' must authorise 'Directed Surveillance' following the procedures detailed in this document for an authorisation to be valid.

2.3 Directed Surveillance Crime Threshold

The Council may only authorise use of directed surveillance under RIPA to prevent or detect criminal offences or prevent disorder involving an offence carrying a maximum term of at least 6 months imprisonment. It can not use directed surveillance incidents that do not involve criminal offences or low level offences such as littering.

The exception is that directed surveillance can be used to prevent or detect specified criminal offences relating to the underage sale of alcohol and tobacco.

- **At the start of an investigation, Officers will need to satisfy themselves that what they are investigating is a criminal offence:**

  Directed surveillance is an invasive technique and at the point it is decided whether or not to authorise its use it must be clear that the threshold is met and that it is necessary and proportionate to use it.

- **An offence with a maximum 6 months imprisonment or more or being related to the underage sale of alcohol and tobacco:**

  Providing the offence under investigation is one which appears on the statute book with at least a maximum 6 months term of imprisonment or is related the underage sale of alcohol and tobacco an application can be made to a Magistrate.

- **During the course of an investigation the type and seriousness of offences may change.**

  If during the investigation it becomes clear that the activity being investigated does not amount to a criminal offence or that it would be a less serious offence that does not meet the threshold, the use of directed surveillance should cease. If a directed surveillance authorisation is already in force it should be cancelled.

Where it is possible, using the evidence obtained, to prove different charges and some are not serious enough the Courts too decide whether to use the evidence and how heavily it is relied upon for the less serious charges.

In addition all other tests & steps must then be met, i.e. that it is necessary and proportionate and where approval from a Magistrate has been granted.

3. Authorisations (See flowchart at Appendix E)

3.1 Applications for directed surveillance

All application forms (**Appendix G**) must be fully completed fully to enable the Authorising Officer to make an informed decision. The point at which they are passed to the Authorising Officer, the Investigating Officer must make sure copies are also sent to the Co-ordinating Officer.

The following information must be included in any application:

- A description of the conduct to be authorised – this must be should be full and detailed, specifying any equipment to be used. The use of maps or sketches to show for example observation posts and target premises should also be considered.
- the purpose of the investigation or operation
- the reason why the authorisation is sought
- the reasons why the surveillance is considered proportionate to what it seeks to achieve
- the nature of the surveillance
- the identities, where known, of those to be the subject of the surveillance
- an explanation or an example of the information which is to be gathered as a result of the operation
- An assessment of Collateral Intrusion (see definition Section 7, page 6)

No authorisation shall be granted unless the Authorising Officer is satisfied that:

- **investigation is necessary** for one of the reasons listed above
- **investigation is proportionate** to the ultimate objective
- it is at an **appropriate** level (i.e. not excessive)
- that the Crime Threshold is met (see above)
- that no other form of investigation would be appropriate.

3.1.1 Urgent Authorisations:

Local Authorities do not have the power to make authorisations, oral or otherwise. All authorisations have to be presented to a Magistrates Court for approval.

3.2 **Granting of Authorisations for directed Surveillance**

Section 32(5) of RIPA requires the Authorising Officers to describe and specify what he is granting. This may or not be the same as requested by the applicant. **Authorised officers must produce a clear description of what is being authorised** in their own words detailing against which subjects, property or location it is authorised. Mere reference to the terms of the application is inadequate.

Authorising Officers must **be careful in the use of 'or' and 'and'** in order not to restrict what is intended. For example, do not use 'or' when 'and' is meant (e.g. deployment of ….on vehicle A or vehicle B' limits deployment to either vehicle, not both simultaneously or one after the other).

Where other subjects may unexpectedly come under surveillance, it can be anticipated by using words such as 'suspected of', 'believed to be' or 'this authority is intended to include conversations between any and all of the subjects of this investigation, including those whose identities are not yet known'.

The Authorising Officer's statement should be **completed in handwriting** as a personal contemporaneous record of the thinking which justified the authorisation. It should set out, in their own words, why he is satisfied or why he believes (RIPA) the activity is necessary and proportionate. A bare assertion is insufficient.

Template entries should be avoided or used with great care as they give the appearance of, minimal or no consideration of the factors, such as necessity and proportionality:

3.2.1 Addressing Necessity

Covert surveillance will not be necessary if the information can reasonably be obtained by overt means. It must also be necessary for the purpose of preventing or detecting crime or of preventing disorder.

Authorising Officers must be satisfied that the use of covert surveillance is necessary for one of the purposes specified in s.28(3) of RIPA. In order to be satisfied, the conduct that it is aimed to prevent or detect must be identified and clearly described, particularly if it is questionable whether serious crime criteria are met. Often missed is an explanation of why it is necessary to use the covert techniques requested – this should be addressed before any authorisation.

3.2.2 Addressing Proportionality:

The person granting the authorisation must also believe that the surveillance is proportionate to what information is being sought by the investigation. This involves balancing the seriousness of the intrusion into the privacy of the subject of the operation (or any other person who may be affected) against the need for the activity in investigative and operational terms meaning:

- the means should not be excessive in relation to the offences being investigated;
- the least intrusive means of surveillance should be chosen; and
- invasion of third parties privacy should, so far as is possible, be minimised; and

The method of surveillance proposed must not be excessive in relation to the seriousness of the matter under investigation. It must be the method which is the least invasive of the target's privacy.

Authorisations must:

- Always be in writing except in urgent cases
- Carefully explain how proportionality has been considered
- Demonstrate how the authorising officer has reached the conclusion that the activity is proportionate to what it seeks to achieve,
- Explain the reasons why the method, tactic or technique proposed is not disproportionate

- Explain why the particular covert method, technique or tactic is least intrusive. It is insufficient to make a simple assertion or to say that the 'seriousness' of the crime justifies any or every method available.
- Explain how and why the methods to be adopted will cause the least possible intrusion on the target and others.
- Explain how and why the activity is an appropriate use of the legislation and the only reasonable way, having considered all others, of obtaining the necessary result, and
- Provide evidence of other methods considered and why they were not implemented.

During and following the authorisation process the Authorising Officer must ensure that copies of all forms and paperwork are passed to the Co-ordinating Officer.

3.2.3 Addressing Collateral intrusion:

Authorising Officers must also take into account the risk of 'collateral intrusion' i.e. intrusion on, or interference with, the privacy of persons other than the subject of the investigation.

Steps must be taken to avoid unnecessary collateral intrusion and minimise any necessary intrusion so as to respect those right to privacy.

Authorisations should state specifically covert activities or techniques likely to be required. It is recognised that it is not always possible, at the outset of any investigation, to foresee how it will progress but techniques shouldn't be authorised where they cannot be demonstrated to be necessary or where they would not be used until the investigation is more mature. Authorising Officers may not authorise more than can be justified at the time.

Those carrying out the investigation must inform Authorising Officers of any unexpected interference with the privacy of individuals who are not covered by the authorisation, as soon as these become apparent.

Where such collateral intrusion is unavoidable, the activities may still be authorised, provided this intrusion is considered proportionate to what is sought to be achieved.

3.2.4 Special consideration in respect of confidential information

Confidential information includes information which is subject to legal privilege, communication between a Member of Parliament and another person on constituency matters, confidential personal information or confidential journalistic material. (ss 98-100 Police Act 1997)

i) **Legal privilege**

Generally, this applies to communications between an individual and their legal adviser in connection with the giving of legal advice in connection with or in contemplation of legal proceedings. Such information is unlikely ever to be admissible as evidence in criminal proceedings.

If in doubt, the advice of the RIPA Co-ordinating Officer should be sought in respect of any issues in this area.

ii) **Confidential personal information**
This is oral or written information held in (express or implied) confidence, relating to the physical or mental health or spiritual counselling concerning an individual (alive or dead) who can be identified from it. Specific examples provided in the codes of practice are consultations between a health professional and a patient, discussions between a minister of religion and an individual relating to the latter's spiritual welfare or matters of medical or journalistic confidentiality.

iii) Confidential journalistic material
This is material acquired or created for the purposes of journalism and held subject to an undertaking to hold it in confidence.

It should be noted that matters considered to be confidential under the Act may not necessarily be properly regarded as confidential under section 41 Freedom of Information Act.

This should only be authorised where there are exceptional and compelling circumstances that make the authorisation necessary.

The following situations must be brought to the inspector/commissioner's attention at the next inspection:

- Where an officer has had to authorise surveillance in respect of an investigation in which he/she is directly involved.
- Where a lawyer is the subject of an investigation or operation;
- Where confidential personal information or confidential journalistic information has been acquired and retained.

3.3 **Applications for CHIS**

The application process is the same as for directed surveillance except that the authorisation must specify the activities and identity of the CHIS and that the authorised conduct is carried out for the purposes of, or in connection with, the investigation or operation so specified.

There are additional requirements in s29(5) of the Act relating to responsibility for dealing with the source and maintenance of records relating to the source.

All application forms (**see Appendix H)** must be fully completed with the required details to enable Authorising Officers to make an informed decision.

There should be a controller, a handler and recorder for a CHIS together with the requirement for a risk assessment if one is to be employed.

In addition to the requirements of the Act the duties set out in the RIPA Source Records Regulations (S.I.2000/2725) must also be observed.

Any officer considering applying for a CHIS should consult the RIPA Co-ordinating Officer before taking any practical steps.

4. Judicial Approval

In order to authorise the use of directed surveillance, acquisition of communications data or use of a CHIS under RIPA, the Council will need to obtain an Order approving the grant or renewal of an authorisation from a Magistrate before it can take effect. If the Magistrate is satisfied that the statutory tests have been met and that the use of the technique is necessary and proportionate he/she will issue an Order approving the grant or renewal for the use of the technique as described in the application.

Judicial approval is in addition to the existing authorisation process. The Council will need to obtain judicial approval for all initial RIPA authorisations/applications and renewals. However there is no requirement for the Magistrate to consider either cancellations or internal reviews.

4.1 Procedure for Applying for Judicial Approval

4.1.1 Making the Application

The flowchart at **Appendix F** outlines the procedure for applying for judicial approval. The application must be made by the Council. Following approval by the Authorising Officer the first stage of the process is for the local authority to contact the Magistrates Court to arrange a hearing.

The Council will need to provide the Magistrate with:

- a copy of the original RIPA authorisation or notice and the supporting documents setting out the case. This forms the basis of the application to the Magistrate and should contain all information that is relied upon. For communications data requests the RIPA authorisation or notice may seek to acquire consequential acquisition of specific subscriber information. The necessity and proportionality of acquiring consequential acquisition will be assessed by the Magistrate as part of their consideration.

- The original RIPA authorisation or notice should be shown to the Magistrate but must be retained by the Council so that it is available for inspection by the Commissioners' offices and in the event of any legal challenge or investigation by the Investigatory Powers Tribunal.

- A partially completed judicial application/order form (**Appendix K**), including a brief summary of the circumstances of the case on the form.

4.2 Attending a Hearing

Council Officers need to be formally designated to appear, be sworn in and present evidence or provide information as required by the Magistrate.

The hearing will be held in private and heard by a single Magistrate who will read and consider the RIPA authorisation or notice and the judicial application/order form. They may have questions to clarify points or require additional reassurance on particular matters.

The investigating Officer will need to answer the Magistrate's questions on the policy and practice of conducting covert operations and detail of the case itself. The investigating Officer will have detailed knowledge of the investigation and will have determined that use of a covert technique is required in order to progress a particular case. This does not, however, remove or reduce in any way the duty of the Authorising Officer to determine whether the tests of necessity and proportionality have been met, Similarly, it does not remove or reduce the need for the forms and supporting papers that the Authorising Officer has considered and which have been provided to the Magistrate to make the case.

The Investigating Officer must ensure all information they intend to use at court have been given to the Authorising Officer, it is not appropriate for the Investigating Officer to rely on new information at this stage.

4.3 **Decision**

The Magistrate will consider whether he/she is satisfied that:

- at the time the authorisation was granted or renewed or the notice was given or renewed, there were reasonable grounds for believing that the authorisation or notice was necessary and proportionate.

- there continues to be reasonable grounds.

- the person who granted the authorisation or gave the notice was an appropriate designated person within the Council; and

- the authorisation was made in accordance with any applicable legal restrictions, for example that the crime threshold for directed surveillance has been met.

The forms and supporting papers must by themselves make the case. It is not sufficient for the local authority to provide oral evidence.

If further information is required to determine whether the authorisation or notice has met the tests then the Magistrate will refuse the authorisation. If an application is refuse the Council should consider whether they can reapply, for example, if there was information to support the application which was available to the Council, but not included in the papers provided at the hearing.

The Magistrate will record their decision on the order section of the judicial application/order form. The Magistrates Court will retain a copy of the Councils RIPA authorisation or notice and the judicial application/order form. This information will be retained securely.

4.4 **Outcomes**

The Magistrate may decide to:

- Approve the Grant or renewal of an authorisation notice, allowing the Council to use the technique in that particular case.

- Refuse to approve the grant or renewal of an authorisation or notice – it will then not take effect and the Council may not proceed. Where an application has been refused the Council may wish to consider the reasons for refusal. For example, a technical error in the form may be remedied without the local authority going through the internal authorisation process again. The Council may then wish to reapply for judicial approval once those steps have been taken.

- Refuse to approve the grant or renewal and quash the authorisation or notice. The court must not exercise its power to quash that authorisation or notice unless the applicant has had at least 2 business days from the date of refusal in which to make representations.

4.5 **Complaints/Judicial Review**

There is no complaint route for a judicial decision unless it was made in bad faith. Any complaints should be addressed to the Magistrates Advisory Committee.

The Council may only appeal a Magistrate decision on a point of law by judicial review.

The Investigatory Powers Tribunal will continue to investigate complaints about the use of RIPA techniques by public bodies, including local authorities. If, following a complaint to them, the Tribunal does find fault with a RIPA authorisation or notice it has the power to quash the Magistrate's order which approved the grant or renewal of the authorisation or notice.

5. Working With/Through Other Agencies

When some other agency has been instructed on behalf of the Council to undertake any action under the Act, this document must be used (as per normal procedure) and the agency advised or kept informed, as necessary, of the various requirements. They must be made aware explicitly what they are authorised to do.

When some other agency (e.g. Police, Customs & Excise, Inland Revenue, etc.):

(a) wish to use the Council's resources (e.g. CCTV surveillance systems), that agency must use its own RIPA procedures and, before any officer agrees to allow the Council's resources to be used for the other agency's purposes, s/he must obtain a copy of that agency's RIPA form for the record (a copy of which must be passed to the RIPA Co-ordinating Officer for the RIPA Central Register) and/or

relevant extracts from the same which are sufficient for the purposes of protecting the Council and the use of its resources;

If the Police or other Agency wish to use Council resources for general surveillance, as opposed to specific RIPA operations, an appropriate letter requesting the proposed use, extent of remit, duration, who will be undertaking the general surveillance and the purpose of it must be obtained from the Police or other Agency before any Council resources are made available for the proposed use. Copies of letters should be sent to the RIPA Co-ordinating Officer for retention.

(b) wish to use the Council's premises for their own RIPA action, the officer should, normally, co-operate with the same, unless there are security or other good operational or managerial reasons as to why the Council's premises should not be used for the agency's activities. Suitable insurance or other appropriate indemnities may be sought, if necessary, from the other agency for the Council's co-operation in the agent's RIPA operation, In such cases, however, the Council's own RIPA forms should not be used as the Council is only 'assisting' not being 'involved' in the RIPA activity of the external agency.

6. Duration of Authorisations and Cancellation

- An authorisation for directed surveillance shall cease to have effect (if not renewed) 3 months from the date of grant or renewal.

- An authorisation for CHIS shall cease to have effect (unless renewed) 12 months from the date of grant or renewal.

- An oral authorisation or renewal shall cease to have effect (unless renewed) 72 hours from the date of grant or renewal

The fact that the operation to which authorisation relates is only expected to last for a short time cannot affect the authorisation period. An early review can take care of issues of continuing necessity and proportionality.

Documentation of any instruction to cease surveillance should be retained and kept with the cancellation form.

When cancelling an authorisation, Authorising Officers should:

1. Record the time and date (if at all) that surveillance took place and the order to cease the activity was made.
2. The reason for cancellation.
3. Ensure that surveillance equipment has been removed and returned.
4. Provide directions for the management of the product.
5. Ensure that detail of property interfered with, or persons subjected to surveillance, since the last review or renewal is properly recorded,
6. Record the value of the surveillance or interference (i.e. whether the objectives as set in the authorisation were met).

A Surveillance Commissioner and Authorising Officers can only authorise on the basis of what they have been told. Issues of disclosure should not inhibit the proper construction of applications and authorisations but can be dealt with at the appropriate time using existing procedures. Where necessary, authorisations should cross-refer to the intelligence report.

7. Reviews & Renewals

Authorising Officers should review all authorisations at regular intervals, as often as necessary and practicable. The reviews should be recorded.

It is a statutory requirement that authorisations are cancelled as soon as they are no longer required. If the proposed operation is expected to be completed quickly, then an early review should take place and Authorising Officers must cancel each authorisation as soon as they decide that the surveillance should be discontinued (s.45 of the Act).

If the directed surveillance authorisation provides for the surveillance of unidentified individuals whose identity is later established, the terms of the authorisation should be refined at review to include the identity of these individuals. It would be appropriate to call a review specifically for this purpose.

Authorising Officers may renew an existing authorisation on the same terms as the original at any time before the original ceases to have effect.

Except in the case of Identities being refined, reviews and renewals should not broaden the scope of the investigation but can reduce its terms.

8. Central Register of Authorisations

The Council must maintain the following documents:

- Copy of the application and a copy of the authorisation together with any supplementary documentation and notification of the approval given by Authorising Officers;
- A record of the period over which the surveillance has taken place;
- The frequency of reviews prescribed by Authorising Officers;
- A record of the result of each review of the authorisation;
- A copy of any renewal of an authorisation and supporting documentation submitted when the renewal was requested;
- The date and time when any other instruction, including to cease surveillance, was given by Authorising Officers.

The RIPA Co-ordinating Officer holds the central register of all authorisations issued by officers. A copy of every application, authorisation, renewal and

cancellation issued should be lodged with them within 2 working days in an envelope marked 'Private and Confidential'.

The Council must also maintain a centrally retrievable record of the following information:

- type of authorisation
- date the authorisation was given
- name and rank/grade of the Authorising Officer
- unique reference number of the investigation/operation
- title (including brief description and names of the subjects) of the investigation/operation;
- whether urgency provisions were used, & if so why
- details of renewal
- whether the investigation/operation is likely to result in obtaining confidential information
- whether the authorisation was granted by an individual directly involved in the investigation
- date of cancellation

These records will be retained for at least 3 years and will be available for inspection by the OSC.

9. Complaints procedure

Contravention of the Data Protection Act 1998 should first be dealt with through the Council's own internal complaints procedure. Information on this is available though the Council's website or through the Democratic Services & Governance Officer. If complainants are unhappy, it may then be reported to the Information Commissioner.

REGULATION OF INVESTIGATORY POWERS ACT 2000

GUIDANCE – PART II

ACQUISITION AND DISCLOSURE OF COMMUNICATIONS DATA

1. Introduction

At this time the Council does not use this power however should the need arise in the future the appropriate appointments to Authorised Officer and SPOC will be made.

Under Chapter I of Part I of Regulation of Investigatory Powers Act ('the Act'), local authorities can authorise the acquisition and disclosure of 'communications data' subject to the tests being met and procedure being followed. Again the Act is supplemented by a Code of Practice **(Appendix I)** ('the Code')

Nothing in this code permits the interception of the content of any communication.

2. What is 'Communications data'?

Communications data is information relating to the use of a communications service e.g. postal service or telecommunications system. It is defined by Section 21(4) of the Act and falls into three main categories: -

Traffic data - where a communication was made from, to whom and when
Service data – use made of service e.g. Itemised telephone records
Subscriber data – information held or obtained by operator on person they provide a service to.

Local authorities are restricted to subscriber and service use data and only for the purpose of preventing or detecting crime or preventing disorder.

3. Application forms

All applications must be made on a standard form (**Appendix J)** and submitted to the single point of contact ("SPOC"). The SPOC will ensure that the application meets the required criteria and then pass to the Designated Person.

4. Authorisations

A Designated Person can only authorise the obtaining and disclosure of communications data if:

(i) it is **necessary** for any of the purposes set out in Section 22(2) of the Act. (The Council can only authorise for the purpose set out in Section

22 (2) (b) which is the purpose of preventing or detecting crime or preventing disorder); and

(ii) it is **proportionate** to what is sought to be achieved by the acquisition of such data (in accordance with Section 22(5) of the Act)

Consideration must also be given to the possibility of **collateral intrusion** and whether any **urgent** timescale is justified.

Once a Designated Person has decided to grant an authorisation or a notice given there are two methods: -

(1) By authorisation of some person in the same relevant public authority as the designated person, whereby the relevant public authority collects the data itself (Section 22(3) of the Act). This may be appropriate in the following circumstances:

- The postal or telecommunications operator is not capable of collecting or retrieving the communications data.
- It is believed 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 communications data.

(2) By notice to the holder of the data to be acquired (Section 22(4) of the Act) which requires the operator to collect or retrieve the data. Disclosure may only be required to either the Designated Person or the single point of contact.

Service provider must comply with the notice if it is reasonably practicable to do so (s.22 (6)-(8) of the Act) and can be enforced to do so by civil proceedings.

Blaby District Council is not permitted to apply or approve orally.

6. Single point of contact ("SPOC")

Notices and authorisations should be passed through a single point of contact within the Council. This should make the system operate more efficiently as the SPOC will deal with the postal or telecommunications operator on a regular basis and also be in a position to advise a designated person on the appropriateness of an authorisation or notice.

SPOCs should be in position to:

- Where appropriate, assess whether access to communications data is reasonably practical for the postal or telecommunications operator;

- Advise applicants and Designated Person on whether communications data falls under section 21(4)(a), (b) or (c) of the Act;

- Provide safeguards for authentication;

- Assess any cost and resource implications to both the public authority and the postal or telecommunications operator.

A SPOC must be accredited which involves undertaking appropriate training.

7. Duration, Renewal and cancellation

Authorisations and notices are only valid for one month beginning with the date on which the authorisation is granted or the notice given. A shorter period should be specified if possible.

An authorisation or notice may be **renewed** at any time during the month it is valid using the same procedure as used in the original application. A renewal takes effect on the date which the authorisation or notice it is renewing expires.

The code requires that all authorisations and notices should be **cancelled** by the Designated Person who issued it as soon as it is no longer necessary, or the conduct is no longer proportionate to what is sought to be achieved. The relevant postal or telecommunications operator should be informed.

8. Retention of records

Applications, authorisations and notices must be retained until the Council has been audited by the Commissioner and to allow the Tribunal (see below) to carry out its functions. A record should be kept of:

- the dates on which the authorisation or notice is started or cancelled.
- any errors that have occurred in the granting of authorisations or giving of notices.

A report and explanation of any errors must also be sent to the Commissioner as soon as is practicable.

10. Oversight and Complaints

The Act provides for an Interception of Communications Commissioner whose remit is to provide independent oversight of the use of the powers contained in Part I and the Code requires any person who uses the powers conferred by Part II to comply with any request made by the Commissioner to provide any information he requires to enable them to discharge thier functions.

The Act also establishes an independent Tribunal to investigate and decide any case within its jurisdiction. Details of the relevant complaints procedure should be available for reference at Blaby District Council's public offices.

APPENDIX A

Code of Practice

Covert Surveillance

See Home Office website:

http://tna.europarchive.org/20100419081706/http://security.homeoffice.gov.uk/ripa/publication-search/general-publications/ripa-cop/covert-surveil-prop-inter-COP

https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/118173/local-authority-england-wales.pdf

APPENDIX B

Code of Practice

Covert Human Intelligence Sources (CHIS)

See Home Office website:

http://tna.europarchive.org/20100419081706/http://security.homeoffice.gov.uk/ripa/publication-search/general-publications/ripa-cop/covert-human-intel-source-COP

APPENDIX C

Office of Surveillance Commissioners

Procedures & Guidance 2010

Please note:

As there is no link to this document on the Office of Surveillance Commissioners' website, it has been placed (as a PDF document – 'Appendix C') with the Council's RIPA Policy and Guidance Notes on the intranet

APPENDIX D

Home Office Guidance

October 2013

See Home Office website:

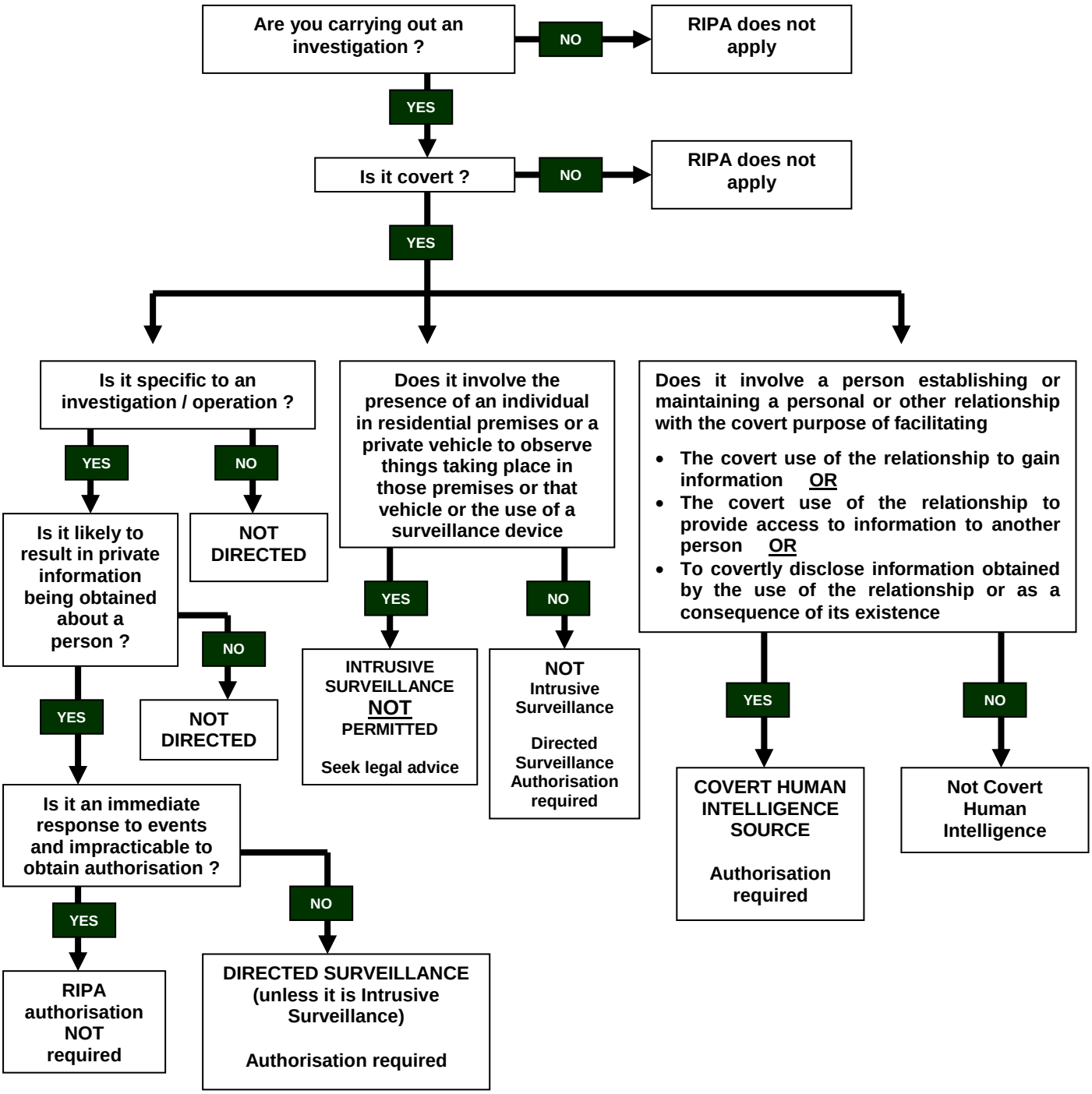
https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/118173/local-authority-england-wales.pdf

APPENDIX E

DIRECTED SURVEILLANCE

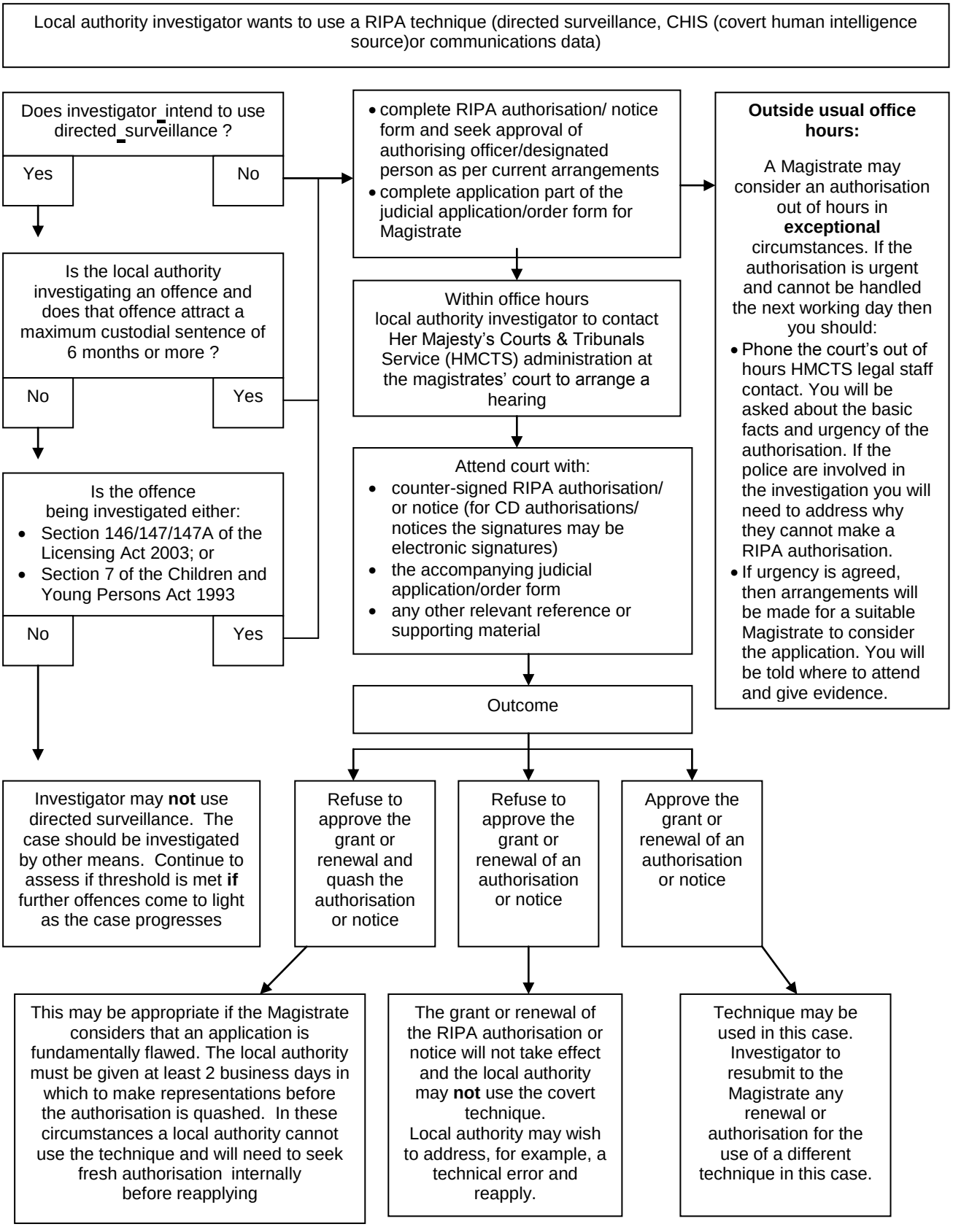
Regulation of Investigatory Powers Act 2000

Do you need Authorisation ?



APPENDIX F

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



APPENDIX G

Forms

Directed Surveillance

APPLICATION

http://tna.europarchive.org/20100419081706/http://security.homeoffice.gov.uk/ripa/publication-search/ripa-forms/application-directed-surveillanc?view=Standard&pubID=690596

REVIEW

http://tna.europarchive.org/20100419081706/http://security.homeoffice.gov.uk/ripa/publication-search/ripa-forms/review-directed-surveillance?view=Standard&pubID=690602

CANCELLATION

Please note:
As the Home Office website does not contain the latest version of the cancellation form, this is attached separately to this document at Appendix I

(Please ensure you remove the words 'APPENDIX I' before printing this form)

RENEWAL

http://tna.europarchive.org/20100419081706/http://security.homeoffice.gov.uk/ripa/publication-search/ripa-forms/renewal-directed-surveillance?view=Standard&pubID=690600

APPENDIX H

Forms

Covert Human Intelligence Sources (CHIS)

APPLICATION
www.security.homeoffice.gov.uk/ripa/publication-search/ripa-forms/chis-application?view=Standard&pubID=447389

REVIEW
www.security.homeoffice.gov.uk/ripa/publication-search/ripa-forms/chis-review?view=Standard&pubID=447372

CANCELLATION
www.security.homeoffice.gov.uk/ripa/publication-search/ripa-forms/chis-cancellation?view=Standard&pubID=447391

RENEWAL
www.security.homeoffice.gov.uk/ripa/publication-search/ripa-forms/chis-renewal?view=Standard&pubID=447370

APPENDIX I

Code of Practice

Co

See Home Office website:

http://tna.europarchive.org/20100419081706/http://security.homeoffice.gov.uk/ripa/publication-search/general-publications/ripa-cop/acquisition-disclosure-cop

APPENDIX J

Forms – Part I

Communications data

APPLICATION
http://www.security.homeoffice.gov.uk/ripa/publication-search/ripa-forms/communications-data.doc?view=Standard&pubID=446995

NOTICE TO COMMUNICATION SERVICE PROVIDER
www.security.homeoffice.gov.uk/ripa/publication-search/ripa-forms/ripa-section-22-notice-update?view=Standard&pubID=590984

APPENDIX K

Unique Reference Number	

Part II of the Regulation of Investigatory Powers Act 2000

Cancellation of a Directed Surveillance authorisation

Public Authority *(including full address)*	

Name of Applicant		**Unit/Branch /Division**	
Full Address			
Contact Details			
Investigation/Operation Name (if applicable)			

Details of cancellation:

1. Explain the reason(s) for the cancellation of the authorisation:

Unique Reference Number	

2. Explain the value of the directed surveillance in the operation:

3. What product has been obtained as a result of the surveillance activity? (You should list here the dates and times of the activity; the nature of the product (i.e., what it shows) and its format (e.g., visual recordings; stills images); associated log/reference numbers; where the product is to be held; and the name of the officer responsible for its future management.) ***nb** – if you have already provided these details in earlier reviews, a cross-reference here should suffice.*

Dates/times	Product obtained	Format & reference numbers	Storage location	Officer responsible

Name (Print) ..... **Grade** .....

Signature ..... **Date** .....

4. Authorising Officer's comments on product obtained. (Paragraph 2.18 of the Covert Surveillance Code of Practice states that arrangements must be in place for the handling, storage and destruction of material obtained through the use of covert surveillance. Authorising Officers must ensure compliance with the appropriate data protection requirements and any relevant codes of practice produced by individual authorities relating to the handling and storage of material. **You should record here how you intend this to be achieved**.)

Unique Reference Number	

5. Authorising Officer's comments on the outcome of this use of directed surveillance and formal cancellation instructions.			
Name (Print)	----------	**Grade**	----------
Signature	----------	**Date and Time**	----------

6. Time and Date when the Authorising Officer instructed the surveillance to cease *(if done verbally prior to this formal written cancellation)*.			
Date:		**Time:**	

APPENDIX L

Application for judicial approval for authorisation to obtain or disclose communications data, to use a covert human intelligence source or to conduct directed surveillance. Regulation of Investigatory Powers Act 2000, sections 23A, 23B, 32A, 32B.

Local authority: ……

Local authority department: ……

Offence under investigation: ……..……..……..

Address of premises or identity of subject: ……..……..

……..……..

……..……..

Covert technique requested: (tick one and specify details)

Communications Data ☐

Covert Human Intelligence Source ☐

Directed Surveillance ☐

Summary of details

……..……..

……..……..

……..……..

……..……..

……

……..……..

Note:
This application should be read in conjunction with the attached RIPA authorisation/RIPA application or notice.

Investigating Officer: ……

Authorising Officer/Designated Person: ……

Officer(s) appearing before Magistrate:……..

Address of applicant department: ……..

……

Contact telephone number: ……

Contact email address (optional): ……..

Local authority reference: ……

Number of pages: ……

Order made on an application for judicial approval for authorisation to obtain or disclose communications data, to use a covert human intelligence source or to conduct directed surveillance. Regulation of Investigatory Powers Act 2000, sections 23A, 23B, 32A, 32B.

Magistrates' court: ……

Having considered the application, I (tick one):

☐ am satisfied that there are reasonable grounds for believing that the requirements of the Act were satisfied and remain satisfied, and that the relevant conditions are satisfied and I therefore approve the grant or renewal of the authorisation/notice.

☐ refuse to approve the grant or renewal of the authorisation/notice.

☐ refuse to approve the grant or renewal and quash the authorisation/notice.

Notes

……

……

……

……

……

Reasons

……

……

……

……

……

……

Signed:

Date:

Time:

Full Name:

Address of magistrates' court: