


|                 |   |  |
|-----------------|---|--|
| Agenda Item No: | 9   |  |
| Committee:      | Corporate Governance  |  |
| Date:           | 19 March 2018   |  |
| Report Title:   | Regulation of Investigatory Powers Act (RIPA) – Policy Update |  |

## 1 Purpose / Summary

- To request that Members consider and make a recommendation to Council to make minor amendments to the Council's RIPA Policy.

## 2 Key issues

- This year the Council had its RIPA policy and procedures inspected by the Investigatory Powers Commissioner's Office (IPCO). This takes place every three years. The IPCO were satisfied with procedures undertaken by the Council in respect of RIPA and recommended some minor adjustments to the RIPA policy. An amended version of this is attached for Members' consideration as **Appendix A**. The changes proposed are highlighted in yellow.

## 3 Recommendations

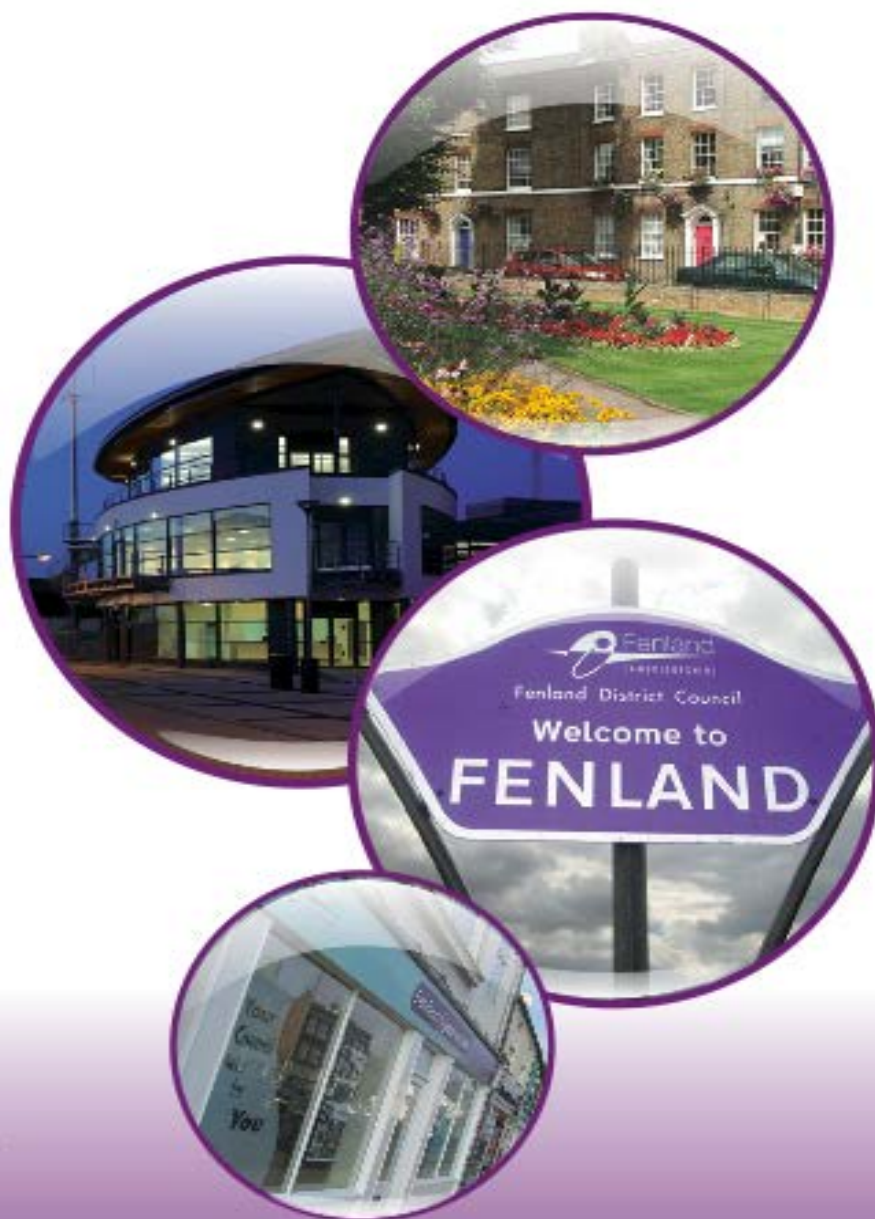
- That Members consider the revised RIPA policy attached to this report and recommend to Council to approve this policy at their meeting on 17 May 2018.

|                               |  |
|-------------------------------|--|
| <b>Wards Affected</b>         | All  |
| <b>Forward Plan Reference</b> | N/A  |
| <b>Portfolio Holder(s)</b>    |  |
| <b>Report Originator(s)</b>   | Geoff Kent – Head of Customer Services   |
| <b>Contact Officer(s)</b>     | Carol Pilson – Corporate Director & Monitoring Officer<br>Geoff Kent – Head of Customer Services |
| <b>Background Paper(s)</b>    | N/a  |

# Regulation Of Investigatory Powers Act (RIPA) Policy

Updated policy, amendments  
are highlighted in yellow

Effective from [date of  
relevant Council]



# Contents

|   |               |
|---|---------------|
| <b>What is this policy about?</b>                             | <b>page 3</b> |
| <b>Introduction</b>   | <b>page 5</b> |
| <b>Part 1 - Directed Surveillance</b>                         |               |
| Definition  | page 8        |
| Authorisation preparation                                     | page 13       |
| Authorisation process   | page 16       |
| Procedure checklist   | page 27       |
| <b>Part 2 - Covert Human Intelligence Sources (or “CHIS”)</b> |               |
| Definition  | page 30       |
| Authorisation preparation                                     | page 32       |
| Authorisation process   | page 35       |
| Procedure checklist   | page 45       |
| <b>Part 3 - Acquisition of Communications Data</b>            |               |
| Definition  | page 46       |
| Authorisation process   | page 48       |
| Procedure checklist   | page 57       |
| <b>Part 4 - General Information</b>                           |               |
| Collaborative Working   | page 62       |
| Record Management   | page 63       |
| Member Oversight  | page 65       |
| Complaints  | page 66       |
| Glossary  | page 67       |
| Annex 1 List of designated Officers and roles                 | page 68       |
| Annex 2 Risk Assessment                                       | page 70       |
| Annex A Home Office RIPA process flowchart                    | page 72       |
| Annex B Approval form for use by Justice of the Peace         | page 73       |

This policy was approved by Council on 18/12/14

Changes proposed drafted 25/1/18 as highlighted, subject to Council approval

# What is this policy about?

## RIPA

The Regulation of Investigatory Powers Act 2000, known as “RIPA” both generally and throughout this policy is the law governing the use of covert techniques by public bodies. It requires that when public bodies need to use covert techniques to obtain private information about someone, they do it in a way that is necessary, proportionate, and compatible with human rights.

## Why do Councils need to use it?

Councils are responsible for enforcing over 100 Acts of Parliament, many of which include offences for which enforcement action can be taken. Some, such as benefit fraud can lead to those found guilty of committing a related offence being sent to prison.

## How must Councils use RIPA?

We use 3 investigatory techniques that can be authorised under RIPA:-

- [Directed surveillance](#),
- Using a [Covert Human Intelligence Source](#) (known commonly as a “CHIS”),
- [Obtaining and disclosing communications data](#).

Since November 2012 local authorities are required to obtain judicial approval prior to using covert techniques. Local authority authorisations and notices under RIPA will only be valid once granted by a Justice of the Peace.

Local authorities can only use RIPA:-

- To prevent and detect conduct which constitutes one or more criminal offences. The criminal offences must be punishable, whether on summary conviction or indictment by a maximum term of at least 6 months imprisonment, or
- Be an offence under-
  - a) S.146 of the Licensing Act 2003 (sale of alcohol to children);
  - b) S.147 of the Licensing Act 2003 (allowing the sale of alcohol to children);
  - c) S.147A of the Licensing Act 2003 (persistently selling alcohol to children);
  - d) S.7 of the Children and Young Persons Act 1933 (sale of tobacco, etc., to persons under eighteen).

## What we do when RIPA does not apply

The RIPA procedure does not apply to:-

- Covert observations where private information will not be obtained.
- Observations that are not carried out covertly.
- Ad-hoc covert observations that do not involve the systematic surveillance of a specific person(s).
- Unplanned observations made as an immediate response to events.

There are situations where surveillance may be required that is not covert and directed. This can apply to cases of:-

- Anti-social behaviour involving disorder.
- Serious internal disciplinary investigations.

The guiding principle is that if surveillance is overt, it does not need RIPA authorisation, i.e.

- Street Scene Officer on patrol.
- Signposted CCTV cameras in normal use.
- Recording noise from outside a property where the occupier has been warned this will happen if the noise continues.
- Conducting test purchases in a matter no different to a member of the public making the same purchase.
- Food Safety or Health and Safety inspections.
- CCTV cameras providing general traffic, crime or public safety information.

Best practice in cases where RIPA does not apply is recommended:-

- A RIPA Authorisation form should be completed and discussed with an Authorising Officer.
- This will ensure that no inappropriate or illegal surveillance takes place.
- It also ensures that a robust and transparent process has been followed before deciding that surveillance is required.

# Introduction

Everyone has a fundamental right to privacy. This means a right not to be watched, have your mail opened or have your personal space invaded. This right is contained in Article 8 of the European Convention on Human Rights:

“Everyone has the right to respect for his private and family life, his home and his correspondence”.

There are times however where the state (including Fenland District Council) can interfere with this right, provided it has a good reason and follows the proper procedures. Accordingly, Fenland District Council may interfere with a person’s right to privacy, if such interference is:-

- In accordance with the law;
- Necessary (as defined in this document); and
- Proportionate (as defined in this document).

The Regulation of Investigatory Powers Act 2000 (‘RIPA’) provides a statutory mechanism (i.e. ‘in accordance with the law’) for authorising ‘[covert surveillance](#)’ and the use of a ‘[covert human intelligence source](#)’ (‘CHIS’) – e.g. undercover agents.

It now also permits public authorities to compel telecommunications and postal companies to obtain and release communications data to themselves, in certain circumstances, known as the “[acquisition of communications data](#)”. It seeks to ensure that any interference with an individual’s right under Article 8 of the European Convention is necessary and proportionate. In doing so, RIPA seeks to ensure both the public interest and the human rights of individuals are suitably balanced.

Directly employed Council staff and external agencies working for Fenland District Council are covered by the Act for the time they are working for Fenland District Council. All external agencies must, therefore, comply with RIPA and the work carried out by agencies on Fenland District Council’s behalf must be properly authorised by one of Fenland District Council’s designated Authorising Officers. Authorising Officers are those whose posts appear in [Appendix 1](#) to this document.

If the correct procedures are not followed, evidence obtained may be disallowed by the courts under the common law, section 78 of the Criminal Evidence Act 1984 and the Human Rights Act 1998.

This means that failure to follow the RIPA rules may mean a criminal prosecution fails and a guilty person is unable to be prosecuted. Furthermore, a complaint of maladministration could be made to the Ombudsman, and/or the Council could be ordered to pay compensation.

Such action would not, of course, promote the good reputation of Fenland District Council and will, undoubtedly, be the subject of adverse media interest. It is essential, therefore, that

all involved with RIPA comply with this document and any further guidance that may be issued, from time to time, by the Monitoring Officer.

Obtaining an authorisation under RIPA and following the procedures in this document, will ensure, therefore, that the action is carried out in accordance with the law and subject to stringent safeguards against abuse of anyone's human rights.

**Note that authorisation to use RIPA must now be in the form of an authorised form signed by a designated Authorising Officer AND formal approval of action by a Justice of the Peace. RIPA cannot be used if only one of these steps have been taken.**

This policy document provides a basic understanding of RIPA and also provides local procedures to ensure compliance. For all officers, either applying to use or tasked with authorising an application for directed surveillance full, authoritative guidance is available in:

The Government website has Codes of Practice relating to RIPA:-  
<https://www.gov.uk/government/collections/ripa-codes>

Local Authority use of RIPA is overseen by an independent regulatory body known as the Investigatory Powers Commissioner's Office, where further information about RIPA is also available:-  
<https://www.ipco.org.uk/>

The Government website has comprehensive guidance on how local authorities can use RIPA since changes to legislation governing its use were made in 2012:-  
<https://www.gov.uk/government/publications/changes-to-local-authority-use-of-ripa>

# **Part 1**

## **Directed Surveillance**



# Directed Surveillance

## Definition

Surveillance, for the purpose of the 2000 Act, includes monitoring, observing or listening to persons, their movements, conversations or other activities and communications. It may be conducted with or without the assistance of a surveillance device and includes the recording of any information obtained.

### Overt surveillance

Most of the surveillance carried out by Fenland District Council will be done overtly – there will be nothing secretive, clandestine or hidden about it. In many cases, Officers will be behaving in the same way as a normal member of the public (e.g. in the case of most test purchases), and/or will be going about Council business openly (e.g. a market inspector walking through markets).

Similarly, surveillance will be overt if the subject has been told it will happen (e.g. where a noisemaker is warned (preferably in writing) that noise will be recorded if the noise continues, or where an 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).

### Covert surveillance

Covert Surveillance is carried out in a manner calculated to ensure that the person subject to the surveillance is unaware of it taking place; i.e. undercover surveillance.

RIPA regulates two types of covert surveillance: Intrusive Surveillance and Directed Surveillance.

### Intrusive surveillance

Intrusive Surveillance is covert surveillance relating to residential premises and private vehicles and involves the presence of a person or device in the actual premises or vehicle of the person/s under surveillance. This might include for example, bugging somebody's telephone or installing a hidden camera in the person's house or car.

Surveillance equipment mounted outside the premises will not be classed as intrusive, unless the device consistently provides information of the same quality and detail as might be expected if they were in the premises or vehicle.

Officers should therefore beware of CCTV recording images through the windows of a person's house and of DAT recorders where they are placed next to a wall and the walls are so thin that the quality of the information recorded were the same as if the DAT recorder had been placed on the other side of the wall.

This form of surveillance can only be carried out by police and other law enforcement agencies. **Council Officers MUST NOT carry out intrusive surveillance.** If you are in any doubt as to whether something amounts to intrusive surveillance, you should talk to a member of the Legal Team.

## Directed surveillance

Surveillance is directed surveillance if the following are all true:

- it is covert, but not intrusive surveillance;
- it is conducted for the purposes of a specific investigation or operation;
- it is likely to result in the obtaining of *private information* about a person (whether or not one specifically identified for the purposes of the investigation or operation);
- It is conducted 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 under Part II of the 2000 Act to be sought.

Thus, the planned covert surveillance of a specific person, where not intrusive, would constitute directed surveillance if such surveillance is likely to result in the obtaining of *private information* about that, or any other person.

## Private information

The officer must decide whether any information about any person's private or family life is likely to be obtained (whether or not that person is specifically targeted for purposes of an investigation).

If the surveillance activities are unlikely to result in the obtaining of private information about a person an authorisation will not be required.

The Codes of Practice state:

*Private information* includes any information relating to a person's private or family life. *Private information* should be taken generally to include any aspect of a person's private or personal relationship with others, including family and professional or business relationships.

Whilst a person may have a reduced expectation of privacy when in a public place, covert surveillance of that person's activities in public may still result in the obtaining of *private information*. This is likely to be the case where that person has a reasonable expectation of privacy even though acting in public and where a record is being made by a *public authority* of that person's activities for future consideration or analysis.

Private life considerations are particularly likely to arise if several records are to be analysed together in order to establish, for example, a pattern of behaviour, or if one or more pieces of information (whether or not available in the public domain) are covertly (or in some cases

overtly) obtained for the purpose of making a permanent record about a person or for subsequent data processing to generate further information. In such circumstances, the totality of information gleaned may constitute *private information* even if individual records do not. Where such conduct includes surveillance, a directed surveillance *authorisation* may be considered appropriate.

*Example: Officers of a local authority wish to drive past a person's home for the purposes of establishing a registration of vehicle on the driveway. Reconnaissance of this nature is not likely to require a directed surveillance authorisation as no private information about any person is likely to be obtained or recorded. However, if the authority wished to conduct a similar exercise, for example to establish a pattern of occupancy of the premises by any person, the accumulation of information is likely to result in the obtaining of private information about that person and a directed surveillance authorisation should be considered.*

*Private information* may include personal data, such as names, telephone numbers and address details. Where such information is acquired by means of covert surveillance of a person having a reasonable expectation of privacy, a directed surveillance *authorisation* is appropriate.

*Example: A surveillance officer intends to record a specific person providing their name and telephone number to a shop assistant, in order to confirm their identity, as part of a criminal investigation. Although the person has disclosed these details in a public place, there is nevertheless a reasonable expectation that the details are not being recorded separately for another purpose. A directed surveillance authorisation should therefore be sought.*

## **Is the surveillance a foreseen or planned response?**

A foreseen or planned response is something other than an immediate response in circumstances where it is not reasonable practicable to get authorisation. An immediate response to events would be for example spotting something suspicious and continuing to observe it.

The regulations no longer allow for the above activities to take place. Authorisation from a Justice of the Peace must always be obtained BEFORE any surveillance can take place.

## **For what purpose can we conduct Directed Surveillance?**

An *authorisation* for directed surveillance by Fenland District Council is only appropriate for the purposes of a specific investigation or operation, insofar as that investigation or operation relates to the grounds specified at section 28(3) of the 2000 Act.

In addition Article 2 of the Regulation of Investigatory Powers (Directed Surveillance and Covert Human Intelligence Sources) (Amendment) Order 2012 inserted a new Article 7A into the Regulation of Investigatory Powers (Directed Surveillance and Covert Human Intelligence Sources) Order 2010. We can only use RIPA:-

- To prevent and detect conduct which constitutes one or more criminal offences. The criminal offences must be punishable, whether on summary conviction or indictment by a maximum term of at least 6 months imprisonment, or
- Be an offence under-
  - a) S.146 of the Licensing Act 2003 (sale of alcohol to children);
  - b) S.147 of the Licensing Act 2003 (allowing the sale of alcohol to children);
  - c) S.147A of the Licensing Act 2003 (persistently selling alcohol to children);
  - d) S.7 of the Children and Young Persons Act 1933 (sale of tobacco, etc., to persons under eighteen).

## Specific situations not requiring directed surveillance authorisation

The following specific activities also constitute neither directed nor intrusive surveillance:

- The recording, whether overt or covert, of an interview with a *member* of the public where it is made clear that the interview is entirely voluntary and that the interviewer is a *member* of a *public authority*. In such circumstances, whether the recording equipment is overt or covert, the *member* of the public knows that they are being interviewed by a *member* of a *public authority* and that information gleaned through the interview has passed into the possession of the *public authority* in question;
- The covert recording of suspected noise nuisance where the intention is only to record excessive noise levels from adjoining premises and the recording device is calibrated to record only excessive noise levels. In such circumstances the perpetrator would normally be regarded as having forfeited any claim to privacy and an *authorisation* may not be necessary;

## General observation activities

The general observation duties of many law enforcement *officers* and other *public authorities* do not require *authorisation* under the 2000 Act, whether covert or overt. Such general observation duties frequently form part of the legislative functions of *public authorities*, as opposed to the pre-planned surveillance of a specific person or group of people.

## Examples of different types of surveillance

| Type of Surveillance   | Examples   |
|--|--|
| <u>Overt</u><br><br>Not requiring prior authorisation                  | <ul style="list-style-type: none"> <li>- Police Officer or Parks Warden on patrol</li> <li>- Signposted Town Centre CCTV cameras (in normal use)</li> <li>- Recording noise coming from outside the premises after the occupier has been warned that this will occur if the noise persists.</li> <li>- Most test purchases (where the officer behaves no differently from a normal member of the public).</li> </ul>   |
| <u>Covert</u><br><br>Not requiring prior authorisation                 | <ul style="list-style-type: none"> <li>- CCTV cameras providing general traffic, crime or public safety information.</li> </ul>  |
| <u>Directed</u><br><br>Must be RIPA authorised                         | <ul style="list-style-type: none"> <li>- Officers follow an individual or individuals over a period, to establish whether they are working when claiming benefit or off long term sick from employment.</li> <li>- Test purchases where the officer has a hidden camera or other recording device to record information which might include information about the private life of a shop-owner, e.g. where they are suspected of selling alcohol or tobacco to under-age customers.</li> <li>- Officers using CCTV for a specific operation or purpose with the intention of obtaining private information, this can include the direction of the Public CCTV system.</li> </ul> |
| <u>Intrusive</u><br><br><b>Fenland District Council cannot do this</b> | <ul style="list-style-type: none"> <li>- Planting a listening or other device (bug) in a person's home or in their private vehicle.</li> <li>- Using the public CCTV system to look inside a person's home, or private vehicle in a planned way.</li> </ul>  |

# Directed Surveillance

## Authorisation Preparation

### General

An authorisation under Part II of the 2000 Act will, providing the statutory tests are met, provide a lawful basis for Fenland District Council to carry out covert surveillance activity that is likely to result in the obtaining of private information about a person.

Accordingly, officers who will be submitting the application and Authorising Officers who will be authorising the application must be familiar with the following information.

**All authorised applications must also be approved by a Justice of the Peace in addition to by the Authorising Officer. Further action in accordance with RIPA can only take place with the approval of a Justice of the Peace.**

### Necessity and proportionality

#### Is the surveillance activity *necessary*?

An authority may **only** be granted by an Authorising Officer if they believe that the use of directed Surveillance is necessary on the grounds of:-

- To prevent and detect conduct which constitutes one or more criminal offences. The criminal offences must be punishable, whether on summary conviction or indictment by a maximum term of at least 6 months imprisonment, or
- Be an offence under-
  - a) S.146 of the Licensing Act 2003 (sale of alcohol to children);
  - b) S.147 of the Licensing Act 2003 (allowing the sale of alcohol to children);
  - c) S.147A of the Licensing Act 2003 (persistently selling alcohol to children);
  - d) S.7 of the Children and Young Persons Act 1933 (sale of tobacco, etc., to persons under eighteen).

#### Is the surveillance activity *proportionate*?

If the activities are deemed necessary, the person granting the *authorisation* must also believe that they are proportionate to what is sought to be achieved by carrying them out. This involves balancing the seriousness of the intrusion into the privacy of the target of the operation (or any other person who may be affected) against the need for the activity in investigative and operational terms.

The *authorisation* will not be proportionate if it is excessive in the overall circumstances of the case. Each action authorised should bring an expected benefit to the investigation or operation and should not be disproportionate or arbitrary. The fact that a suspected offence may be serious will not alone render intrusive actions proportionate. Similarly, an offence may be so minor that any deployment of covert techniques would be disproportionate. No activity should be considered proportionate if the information which is sought could reasonably be obtained by other less intrusive means.

The following elements of proportionality should therefore 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 target and others;
- considering whether the activity is an appropriate use of the legislation and a reasonable way, having considered all reasonable alternatives, of obtaining the necessary result;
- Evidencing, as far as reasonably practicable, what other methods had been considered and why they were not implemented.

*Example 1: An individual is suspected of claiming a false address in order to abuse a school admission system operated by his local education authority. The local authority considers it necessary to investigate the individual for the purpose of preventing or detecting crime. Although these could be legitimate grounds for seeking a directed surveillance authorisation, if the individual's actions were capable of constituting a crime, such surveillance is unlikely to be necessary or proportionate to investigate the activity. Instead, it is likely that other less intrusive, and overt, means (such as unscheduled visits to the address in question) could be explored to obtain the required information.*

*Example 2: An individual is suspected of a relatively minor offence, such as littering, leaving waste out for collection a day early, or permitting dog-fouling in a public place without clearing up afterwards. It is suggested that covert surveillance should be conducted against her to record her movements and activities for the purposes of preventing or detecting crime, or preventing disorder. Although these could be legitimate grounds for seeking a directed surveillance authorisation, if the individual's actions were capable of constituting an offence or disorder, strong consideration should be given to the question of proportionality in the circumstances of this particular case and the nature of the surveillance to be conducted. In particular, the obtaining of private information on the individual's daily routine is unlikely to be necessary or proportionate in order to investigate the activity of concern. Instead, other less intrusive means are likely to be available, such as general observation of the location in question until such time as a crime may be committed. In addition, it is likely that such offences can be tackled using overt techniques.*

## **Collateral intrusion**

Before authorising applications for directed surveillance, the Authorising Officer should also take into account the risk of obtaining private information about persons who are not subjects of the surveillance or property interference activity.

Measures should be taken, wherever practicable, to avoid or minimise unnecessary intrusion into the privacy of those who are not the intended subjects of the surveillance activity. 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. The same proportionality tests apply to the likelihood of collateral intrusion as to intrusion into the privacy of the intended subject of the surveillance.

All applications should therefore include an assessment of the risk of collateral intrusion and details of any measures taken to limit this, to enable the Authorising Officer to fully consider the proportionality of the proposed actions.

## **Confidential material**

Special consideration must also be given to authorisations that involve confidential personal information, confidential constituent information and confidential journalistic material.

Confidential information consists of matters subject to legal privilege, confidential constituent information, confidential personal information or confidential journalistic material.

If the directed surveillance is likely to result in the acquisition of confidential material the Authorising Officer must have full consideration of this in assessing whether the surveillance activities are proportionate. Applications in which surveillance activities are likely to result in the acquisition of confidential material will only be considered in the most exceptional and compelling circumstances.

Where there is any doubt as to the handling and dissemination of confidential information, advice should be sought from Legal Services before any further dissemination of the material takes place.

Only the Chief Executive (or the Monitoring Officer, but only if the Chief Executive is absent) has the authority to authorise surveillance where it is likely to result in the acquisition of confidential information.

Where such material has been acquired and retained, the matter should be reported to the relevant Commissioner or Inspector during his next inspection and the material be made available to him if requested.



# Directed Surveillance Authorisation Process

The authorisation forms are standard forms available from the RIPA Coordinator. There are a number of stages to then go through, as set out in the following pages, before the directed surveillance can commence; it can never do so without being formally approved by a Justice of the Peace. The form to then be used when applying to a Justice of the Peace is attached to this policy as [Annex B](#).

These forms should be completed and submitted for authorisation as early as possible prior to the start of the proposed surveillance activity. This is to allow for the need to gain authorisation from a Justice of the Peace.

Furthermore, once the authorisation is given by a Justice of the Peace, there should be no delay in beginning the surveillance activity. Any delay may result in the circumstances changing and the authorisation being out of date.

If there is any deviation from the above, officers must check and ensure that the circumstances of the investigation have not changed before obtaining authorisation and/or beginning the surveillance activity. Where there has been a change in circumstances the authorisation will need to be revised before it is submitted or the authorisation reviewed if authorisation has already been given.

## Applications for authorisation for Directed Surveillance - How the form must be completed by the Investigating Officer

This section sets out what the Investigating Officer needs to consider and cover when completing the authorisation form.

### Unique Reference Number (URN)

Each application form will have a Unique Reference Number (URN) as follows: -

*Year/Service\*/Type of authorisation\*\*/Number\*\*\**

2010/EP/DS/0001

\*The services are as follows: -

Environmental Protection (EP), Environmental Health (EH), Environmental Services (ES), Planning (P), Housing (H), Fraud (F), Anti-Social Behaviour (ASB,) Building Control (BC), Internal Audit (IA)

\*\*Directed surveillance (DS)

(Please note that this is here for identification purposes only and will have no bearing on the numbering.)

\*\*\*Each service shall start at 0001 and run consecutively irrespective of the type of authorisation.

The RIPA Co-ordinator shall issue the relevant URN to Investigating Officers. This URN shall identify the particular operation and should be cross referenced on associated review, renewal and cancellation forms. Please note that where more than one application is required within any particular investigation, each application shall have its own URN.

Rejected forms will also have their own URN's.

The cross-referencing of each URN takes place within the various forms for audit purposes.

#### Section 1 - Rank and Position of the Authorising Officer

- Please note that the exact position of the Authorising Officer should be given.

#### Section 2 – Describe the purpose of the investigation or operation

- Specify what you want to do and why;
- Provide details of the investigation and enquiries to date;
- State your objectives of the investigation and the surveillance, which should fit in with what you are asking to be authorised;

#### Section 3 – Provide details of the surveillance operation to be authorised and expected duration, including any premises, vehicles or equipment that may be used

- The type of surveillance, e.g. static or foot mobile surveillance;
- What is being surveyed, e.g. address and details of any premises or vehicles if known;
- When will the surveillance take place, certain times, 24 hours a day etc.?
- Equipment to be used, e.g. camera, video, CCTV, recording equipment, binoculars etc.;

**Remember that you can only do what you are authorised to do so you need to be as thorough and as detailed as possible in this section.**

#### Section 4 – Provide the identities, where known, of those to be subject of the directed surveillance

- Name;
- Address;
- DOB;
- Other information as appropriate;
- Description, associates etc. where names are not known.

#### Section 5 – Provide the information that is desired to obtain as a result of the directed surveillance

For example: -

- To identify location of subjects place of work;
- To assist in establishing whether the employer is also involved;
- To gather intelligence and evidence to establish extent of criminality;
- To identify other persons involved;
- To identify other premises involved;
- To identify the method of operation;
- To obtain the best evidence to assist with prosecution of offenders;
- To obtain the best evidence with regards to the identification of persons responsible etc.

#### Section 6 – Provide the grounds under which the directed surveillance is necessary

This will **always** be for only these circumstances:-

- To prevent and detect conduct which constitutes one or more criminal offences. The criminal offences must be punishable, whether on summary conviction or indictment by a maximum term of at least 6 months imprisonment, or
- Be an offence under-
  - a) S.146 of the Licensing Act 2003 (sale of alcohol to children);
  - b) S.147 of the Licensing Act 2003 (allowing the sale of alcohol to children);
  - c) S.147A of the Licensing Act 2003 (persistently selling alcohol to children);
  - d) S.7 of the Children and Young Persons Act 1933 (sale of tobacco, etc., to persons under eighteen).

## Section 7 – Explain the reasons why the directed surveillance is necessary on the grounds specified

- State that you suspect a criminal offence is being committed, what it is, and if known, what legislation you suspect it is being committed under.
- Also include reasons why it is necessary to use directed surveillance, for example: -
  - Other methods of evidence/intelligence gathering have been tried and failed;
  - Overt enquiries will lead to the subject knowing of the investigation and hamper the evidence gathering process;
  - Only way to identify the perpetrator etc.

## Section 8 – Provide details of any potential collateral intrusion, why the intrusion is unavoidable and precautions that will be taken to minimise collateral intrusion

- Describe the scene, and where necessary attach a plan or a map etc.
- There will be collateral intrusion on neighbours, family members, members of the public, other employees, other customers etc.
- State why the collateral intrusion is unavoidable, e.g. it is the only location available to carry out the observations, the methods used are the only available options etc.
- Details of how the collateral intrusion will be kept to a minimum, e.g. by using sufficiently trained staff to achieve the objectives, by focusing the surveillance on the designated subject/locations with set objectives thereby reducing/minimizing collateral intrusion, the surveillance activity will cease once the surveillance objectives are achieved etc., photographic equipment will only be used for the evidence and intelligence gathering purposes and will focus on the subject/activity taking place etc.
- All information will be recorded and retained in accordance with DPA and CPIA principles.

## Section 9 – Explain the reasons why the surveillance is considered proportionate to what it seeks to achieve

Are you asking to do a lot to achieve a little? Do not use a sledgehammer to crack a nut. In considering the proportionality, you should consider the following (this list is not exhaustive):

-

- Serious nature of offence;
- Prevalence of type of offence;
- Impact on victims;
- If not authorised offences may continue without the required evidence to prosecute the offender;
- Surveillance will ultimately lead to prosecution of offender;
- Insufficient evidence to prosecute
- Deterrent effect of prosecution on perpetrator and wider public;
- Our responsibility to the public and environment etc.;
- Our responsibility to the public purse?
- What is the cost of the criminal activity to the Council and ultimately the public? Specify figures where available.
- Community safety;
- Crime rate;
- Economy of local area;
- Other methods of evidence/intelligence gathering have been tried and failed;
- Overt enquiries will lead to the subject knowing of the investigation and hamper the evidence gathering process;
- May reduce additional collateral intrusion by shortening the length of the investigation;
- Consequences of not taking any action are.....;

## Section 10 – Confidential Information

- Identify how likely, and if so, what type of confidential information may be acquired as a result of the directed surveillance.

Please note that where there is a likelihood of acquiring confidential information, the form will need to be submitted to the Chief Executive for authority.

## Section 11 – Applicants details

This is self-explanatory.

Section 12 onwards must be completed by the Authorising Officer.

Before taking the form to the Authorising Officer, the Investigating Officer must take the form completed up to and including Section 11 back to the RIPA Coordinator, for them to satisfy themselves that it is completed correctly and can now be taken to the Authorising Officer.

Once the RIPA Coordinator is satisfied, they will give the partially completed form back to the Investigating Officer who will then take it to the Authorising Officer, who will then follow the next part of the process as set out below.

## **Application for authorisation for Directed Surveillance - Authorisation procedures for Authorising Officers**

Responsibility for authorising the carrying out of directed surveillance rests with the Authorising Officer and requires the personal authority of the Authorising Officer. The Regulation of Investigatory Powers (Directed Surveillance and Covert Human Intelligence Sources) Order 2010 designates the required level of office for each Authorising Officer.

**Only** those named officers authorised under this policy to be 'Authorising Officers' for the purpose of RIPA can authorise directed surveillance. See Appendix 1 – List of Authorising Officers. No other Officers can give approval.

An Authorising Officer **must only** give authorisations in writing.

Authorising Officers must have received appropriate training. If an Authorising Officer has not received appropriate training, they **cannot** approve/reject any action set out in this policy.

Authorising Officers **must exercise their minds every time they are asked to sign a form**. They must never sign or rubber stamp Form(s) without thinking about their personal and Fenland District Council's responsibilities. It is not acceptable to use "copy and paste" from previous forms; each application must be individually and carefully considered.

An Authorising Officer should not authorise directed surveillance where they are actively involved in the investigation for which it is required. Accordingly, authority should be provided by an alternative Authorising Officer (it does not matter if they are from a different service).

#### Section 12 – Authorising Officers Statement

You need to spell out the “5 W’s – Who, What, Where, When, Why and How”: -

- Why the surveillance is necessary;
- Whom is the surveillance directed against;
- Where it will take place;
- When it will take place;
- What surveillance activity/equipment is sanctioned;
- How it is to be achieved?

It is essential that you are clear about what you are authorising and why you are authorising it. It is not sufficient to refer to previous sections of the form, to leave the section blank or insert responses such as ‘ok, no’.

#### Section 13 – Authorising Officer – Necessity and Proportionality

You need to state in your own words why you believe the directed surveillance is necessary (i.e. justify that it is for the prevention/detection of crime and disorder) and why you believe it to be proportionate to what is being sought by carrying it out.

#### Section 14 – Confidential Information Authorisation

If there is a likelihood of acquiring confidential information you should supply detail that demonstrates compliance with the Codes of Practice

#### Date of first Review/Programme for Subsequent Reviews

The Authorising Officer must set a date for review of the authorisation and review on that date; please see notes on reviews below.

## Approval by a justice of the peace (JP)

Once Surveillance has been authorised as detailed above, the Authorising Officer will pass the completed authorisation to the RIPA Coordinator for consideration, acting as an independent check at that time.

The RIPA Coordinator **must** contact the Court to apply for approval from a JP using the prescribed form shown at [Annex B](#) of this report. In addition [Annex A](#) shows a flowchart of the application process.

They will need to arrange a hearing for the application to be heard, **which the Authorising Officer will attend with:-**

- RIPA authorisation form signed by an Authorising Officer,
- The accompanying Judicial application form,
- All other relevant documents (sufficient supporting information that will allow the JP to make a fully informed decision).

At the hearing the JP will:-

- Refuse to grant the surveillance, in which case the process must stop and the Council seek fresh approval internally and at Court with more detailed information,
- Grant approval to undertake the surveillance.

## After approval by a JP

The directed surveillance can take place as authorised subject to the time restrictions placed on it. When it expires, it must be renewed by completing the full application process above including gaining approval from a JP.

## Urgent oral authorisations

These are not permitted under any circumstances.

## Duration

The 'authorisation' to carry out/conduct the surveillance is only valid for three months from the date on which a Justice of the Peace has approved the authorised RIPA application to 23:59 on the day that is the last day of the three months starting from the first day of this period for Directed Surveillance.

## Reviews



Regular reviews of the authorisations should be undertaken to assess the need for surveillance to continue. Furthermore, any change in circumstances will prompt the need for a review to be carried out. There is a standard form available for this purpose which is available from the Legal team.

In each case the frequency of reviews should be considered at the outset by the Authorising Officer. This should be as frequently as is considered necessary and practicable. Particular attention is drawn to the need to review authorisations frequently where the surveillance or property interference involves a high level of intrusion into private life or significant collateral intrusion, or confidential information is likely to be obtained.

The Investigating Officer should complete the form and submit to the Authorising Officer in time for it to be signed on the date specified on the original application or previous review. The sections are similar to that on the original authorisation form and accordingly the same principles should be applied.

The results of the review must be recorded on the central record of authorisations and on the service's own record of authorisations. They should be retained for at least 3 years.

Any proposed or unforeseen changes to the nature or extent of the surveillance operation that may result in the further or greater intrusion into the private life of any person should also be brought to the attention of the Authorising Officer by means of a review. The Authorising Officer should consider whether the proposed changes are proportionate (bearing in mind any extra intended intrusion into privacy or collateral intrusion), before approving or rejecting them. Any such changes must be highlighted at the next renewal if the authorisation is to be renewed.

Where a directed surveillance authorisation provides for the surveillance of unidentified individuals whose identity is later established, the terms of the authorisation should be refined at a review to include the identity of these individuals. It would be appropriate to convene such a review specifically for this purpose. This process will not require a fresh authorisation, providing the scope of the original authorisation envisaged surveillance of such individuals. Such changes must be highlighted at the next renewal if the authorisation is to be renewed.

## **Renewals**

An authorisation can be renewed before it ceases to have effect if an Authorising Officer considers it necessary for the authorisation to continue. The renewal takes effect at the time at which the authorisation would have ceased to have effect. If necessary a renewal can be made more than once. A written renewal may authorise the directed surveillance for a further 3 months.

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

Renewals should be made in writing on the appropriate form; there is a standard form available for this purpose from the Legal team.

Renewal forms should be completed and submitted for authorisation up to 3 days prior to the expiry of the proposed surveillance activity and **no longer**. Any longer than this and it is likely that the circumstances set out in the form will have changed and any authorisation will be out of date.

If there is any deviation from the above, Investigating Officers must check and ensure that the circumstances of the investigation have not changed before obtaining authorisation for a renewal. Where there has been a change in circumstances the application for renewal will need to be revised before being submitted to the Authorising Officer.

The sections are similar to that on the original authorisation form and accordingly the same principles should be applied.

A renewal must be recorded on the central record of authorisations and on the service's own record of authorisations.

A renewal **must** be submitted for approval by, and approved by a Justice of the Peace before it can be put into operation.

## Cancellations

The Authorising Officer who granted or last renewed an authorisation must cancel the authorisation if the grounds for granting the authorisation no longer apply, i.e. the aims have been met or the risks/circumstances have changed and the current authorisation is no longer appropriate.

As soon as the decision is taken that directed surveillance should be discontinued, the instruction must be given to those involved to stop all surveillance of the subject(s). The date the *authorisation* was cancelled should be centrally recorded and documentation of any instruction to cease surveillance should be retained. There is no requirement for any further details to be recorded when cancelling a directed surveillance *authorisation*.

There is a standard form available for this purpose from the Legal team. Once completed these forms must be kept on the central record of authorisations and on the service's own record of authorisations.

The Authorising Officer must inform those involved in the surveillance to stop all surveillance of the subject(s).

It is good practice for individual service's within the Council to maintain an index detailing the product obtained from the surveillance and whether or not objectives were achieved.

The cancellation does not need to be advised or approved by a Justice of the Peace.

## Keeping of records

### Centrally retrievable records of Directed surveillance authorisations

A record of the following information pertaining to all authorisations shall be centrally retrievable within the Council for a period of at least three years from the ending of each authorisation. This information should be regularly updated whenever an authorisation is granted, renewed or cancelled and should be made available to the relevant Commissioner or an Inspector from the Office of Surveillance Commissioners upon request.

- the type of authorisation;
- the date the authorisation was given;
- name and rank/grade of the Authorising Officer;
- the unique reference number (URN) of the investigation or operation;
- the title of the investigation or operation, including a brief description and names of subjects, if known;
- if the authorisation has been renewed, when it was renewed and who authorised the renewal, including the name and rank/grade of the Authorising Officer;
- whether the investigation or operation is likely to result in obtaining confidential information as defined in this code of practice;
- whether the authorisation was granted by an individual directly involved in the investigation;
- the date the authorisation was cancelled.

The following documentation should also be centrally retrievable for at least three years from the ending of each authorisation:

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

# Directed Surveillance Procedure Checklist

The basic procedure for obtaining authorisation for directed surveillance is as follows:-

- The Investigating Officer having considered the aim of the surveillance, the type of surveillance and equipment required (including establishing that the equipment is available for the duration of the anticipated surveillance), the requirements of necessity, proportionality and collateral intrusion (including carrying out a risk assessment) shall contact the RIPA Coordinator to obtain an authorisation form.
- They shall then seek agreement from the RIPA Coordinator to proceed, and then submit the form to the Authorising Officer (no more than 3 days prior to the anticipated commencement of the surveillance activity).
- The Authorising Officer shall consider the requirements of necessity, proportionality and collateral intrusion and if satisfied shall authorise the form for 3 months, noting that the authorisation will apply from the date on which a Justice of the Peace approves the authorisation.
- The Authorising Officer shall provide a copy of the application whether rejected or authorised to the Investigating Officer and to the RIPA Coordinator for a final check and sign-off, the letter will also place a copy on the central file.
- If satisfied the RIPA Coordinator will liaise with the Court to arrange for the Authorising Officer to attend Court to seek approval for surveillance to commence.
- The Authorising Officer will make an application to a Justice of the Peace using the form at Annex B of this policy. Only once the Justice of the Peace gives approval, can the matter proceed.
- In order to make the required application to a Justice of the Peace, the Authorising Officer must be properly authorised to do so under section 223 of the Local Government Act 1972.
- At the time of authorisation the Authorising Officer shall set a date for a review (not more than 1 month from the date of the authorisation, more frequent where required).
- The Investigating Officer shall commence the surveillance once authorised.
- Not more than 3 days prior to the date for review (or where there has been a change of circumstances) the Investigating Officer shall complete and submit the review form to the Authorising Officer.
- If satisfied that the surveillance activity is still necessary and proportionate, the Authorising Officer shall sign off the review form and set a further date for review.

- The Authorising Officer shall provide a copy of the review form whether rejected or authorised to the Investigating Officer and the Head of Service and send the original to the RIPA Coordinator and Monitoring Officer (central file).
- If, when the Authorisation is near to expiry, a renewal is deemed necessary, the Investigating Officer shall complete the renewal form, and in doing so shall carry out the same considerations as for the initial application, and additionally include the value of the surveillance activity to date.
- They shall submit the renewal form to the Authorising Officer not more than 3 days prior to the expiry of the previous authorisation.
- The Authorising Officer shall consider the requirements of necessity, proportionality and collateral intrusion and if satisfied shall authorise the form for a duration appropriate to the individual circumstances of the case (but not more than 3 months).
- At this point the Investigating Officer must again make an application to a Justice of the Peace using the form at Annex B of this policy. Only once the Justice of the Peace gives approval, can the matter proceed.
- The Authorising Officer shall provide a copy of the renewal whether rejected or authorised to the Investigating Officer and the Head of Service and send the original to the Monitoring Officer (central file).
- At the time of the renewal the Authorising Officer shall set a date for a review (not more than 1 month from the date of the authorisation, less if necessary) and the process as above shall continue.
- Once the surveillance activity is complete or the time authorised time period has expired the Investigating Officer shall complete a cancellation form which they shall submit to the Authorising Officer.

## **Part 2**

# **Covert Human Intelligence Sources or “CHIS”**

# CHIS

## Definition

### Who is a CHIS?

A Covert Human Intelligence Source (CHIS) is someone who establishes or maintains a personal or other relationship for the covert purpose of obtaining or providing access to information and covertly disclosing information obtained by the use or as a consequence of that relationship. This includes someone who volunteers information to us on a repeated basis. We must keep such sources under constant review to ensure that they are managed with an appropriate level of sensitivity and confidentiality, and to establish whether, at any given stage, they should be authorised as a CHIS.

A CHIS may include an informant, agent or officers working undercover.

The purpose is covert in relation to the establishment or maintenance of a personal or other relationship if the relationship is conducted in a way that is calculated to ensure that one of the parties to that relationship is unaware of the purpose.

Furthermore, a relationship is used covertly and information used or disclosed covertly if the information used or disclosed is done so in such a manner that is calculated to ensure that one of the parties does not know of the use or disclosure of information.

Accordingly, where a member of the public obtains information in the normal course of their life, trade or business or of suspected criminal activity and they are receiving no extra reward or direct they will not need to be recorded as a CHIS. Therefore, RIPA does not apply in circumstances where members of the public volunteer information to Fenland District Council as part of their normal civic duties, or to contact numbers set up to receive information. **Please see next paragraph regarding repeat information giving.**

**A member of the public may in reality be a CHIS when giving the Council information where information passed to the Council is done so during the course of or consequence of a personal or other relationship. When an informant gives repeat information, Officers should seek guidance from the RIPA Coordinator as to whether RIPA applies before acting upon information used from the informant.**

Further guidance about the definition and use of a CHIS is on the Government website:-  
<https://www.gov.uk/government/publications/draft-ripa-codes-of-practice-covert-human-intelligence-sources-covert-surveillance-and-property-interference>

## What must be authorised?

The Conduct or Use of a CHIS requires prior authorisation.

- **Use** of a CHIS is the actions of inducing, asking or assisting a person to act as a CHIS.
- **Conduct** of a CHIS is the establishing or maintaining a personal or other relationship with a person for the covert purpose of (or is incidental to) obtaining and passing on information.

## Juvenile CHIS

Special safeguards apply to the use or conduct of juvenile sources (i.e. under 18 year olds). On no occasion can a child under 16 years of age be authorised to give information against his or her parents. Advice should be sought from the Monitoring Officer.

The duration of such an authorisation is **one month** instead of twelve months for a normal CHIS authorisation.

## Vulnerable individuals

A Vulnerable Individual is a person who is or may be in need of community care services by reason of mental or other disability, age or illness and who is or may be unable to take care of himself or herself, or unable to protect himself or herself against significant harm or exploitation.

A Vulnerable Individual will only be authorised to act as a source in the most exceptional of circumstances. Advice should be sought from the Monitoring Officer.



# CHIS

## Authorisation Preparation

The use of a CHIS can only be lawfully carried out if properly authorised, and in strict accordance with the terms of the authorisation.

For an authorisation for the use or conduct of a CHIS to be granted the Authorising Officer must be satisfied that the use or conduct is:-

- In accordance with the law;
- Necessary; and
- Proportionate.

**All authorised applications must also be approved by a Justice of the Peace in addition to by the Authorising Officer. Further action in accordance with RIPA can only take place with the approval of a Justice of the Peace.**

### In accordance with the law

RIPA provides a statutory mechanism that makes certain interference with a person's private life in accordance with the law, including, the use and conduct of a CHIS.

### Necessary

An authority may only be granted by an Authorising Officer if they believe that the conduct and use of the CHIS is necessary after satisfying themselves that this is appropriate with reference to CHIS guidance as referred to on page 29 of this Policy.

### Proportionality

If the conduct or use of a CHIS is necessary for the prevention or detection of crime or disorder the Authorising Officer must then go on to consider whether or not the proposed use or conduct of a CHIS is proportionate. In considering proportionality, the Authorising Officer should consider the following:

- The means should not be excessive by relation to the gravity of the mischief being investigated. More simply put, what is sought to be achieved from the conduct or use of a CHIS? It will only be proportionate to carry out surveillance activities if they are not excessive in relation to what is trying to be achieved.
- The least intrusive means should be chosen; and

- Take into account the risk of intrusion into the privacy of persons other than the specified subjects in the use and conduct of the CHIS: 'collateral intrusion' (see below). Measures must be taken wherever practicable to avoid or minimise, so far as is possible, collateral intrusion.
- Special consideration should be given where any activity is likely to result in the acquisition of confidential material.

## Collateral Intrusion

Collateral intrusion is where there is a risk of intrusion into the privacy of persons other than those who are directly the subjects of the investigation or operation.

Before authorising the use or conduct of a CHIS, the Authorising Officer must consider the risk of collateral intrusion and whether a separate authorisation is required for any collateral intrusion or interference with the privacy of persons other than the subject(s) of the operation or investigation. Measures should be taken, wherever practicable, to avoid unnecessary intrusion into the lives of those not directly connected with the operation.

An application for an authorisation should include an assessment of the risk of any collateral intrusion. A suggested risk assessment for this purpose can be found at appendix 2. The Authorising Officer should take this into account, when considering the proportionality of the use and conduct of a source.

Those managing the operation should inform the by way of a review Authorising Officer if the investigation or operation unexpectedly interferes with the privacy of individuals not covered by the authorisation. The Authorising Officer must then consider whether the current authorisation is sufficient or a new authorisation is required.

## Confidential Material

Confidential information consists of matters subject to legal privilege, confidential personal information or confidential journalistic material. If the conduct or use of any CHIS is likely to result in the acquisition of confidential material the Authorising Officer must have full consideration of this in assessing whether use or conduct of the CHIS is proportionate.

Applications in which the use or conduct of a CHIS is likely to result in the acquisition of confidential material will only be considered in exceptional and compelling circumstances and the Authorising Officer must give the fullest consideration to any such cases. Applications in which the conduct or use of a CHIS are likely to result in the acquisition of confidential material will only be considered in the most exceptional and compelling circumstances.

Only the Chief Executive has authority to authorise the use or conduct of a CHIS where it is likely to result in the acquisition of confidential material, except in **exceptional circumstances** where the Chief Executive is absent; when the Monitoring Officer can authorise this.

## **Additional Safeguards when Authorising a CHIS**

When authorising the conduct or use of a CHIS, an Authorising Officer must also be satisfied that appropriate arrangements are in place for the management and oversight of the CHIS and that any health and safety issues have been addressed. Accordingly, as part of the application process the Investigating Officer shall carry out a risk assessment.

Any person granting or applying for an authorisation will also need to be aware of any particular sensitivities in the local community where the source is being used and of similar activities being undertaken by other public authorities which could impact on the deployment of the source. Consideration should also be given to any adverse impact on community confidence or safety that may result from the use or conduct of a source or of information obtained from that source.

Officers must ensure that records of the CHIS contain particulars and are not available except on a need to know basis.

# CHIS

## Authorisation Process

The authorisation forms are standard forms are available from the RIPA Coordinator. There are a number of stages to then go through, as set out in the following pages, before the directed surveillance can commence; it can never do so without being formally approved by a Justice of the Peace. The form to then be used when applying to a Justice of the Peace is attached to this policy as [Annex B](#).

These forms should be completed and submitted for authorisation as early as possible prior to the start of the proposed surveillance activity. This is to allow for the need to gain authorisation from a Justice of the Peace.

Furthermore, once an authorisation is given, there should be no delay in beginning the conduct or use of the CHIS as this may result in the circumstances changing.

If there is any deviation from the above, the Investigating Officer must check and ensure that the circumstances of the operation have not changed before obtaining authorisation and/or beginning the use or conduct the CHIS. Where there has been a change in circumstances the authorisation will need to be revised before it is submitted and the authorisation reviewed if authorisation has been given.

### **Applications for authorisation for use of a CHIS - How the form must be completed by the Investigating Officer**

This section sets out what the Investigating Officer needs to consider and cover when completing the authorisation form.

#### Unique Reference Number (URN)

Each application form will have a Unique Reference Number (URN) as follows: -

Year/Service\*/Type of authorisation\*\*/Number\*\*\*

\*The Services are as follows: -

Environmental Protection (EP), Environmental Health (EH), Environmental Services (ES), Planning (P), Housing (H), Fraud (F), Anti-Social Behaviour (ASB,) Building Control (BC), Internal Audit (IA)

\*\*Covert Human Intelligence Source (CHIS)

Please note that this is here for identification purposes only and will have no bearing on the numbering.

\*\*\*Each service shall start at 0001 and run consecutively, irrespective of the type of authorisation sought.

Examples: -

2006/EP/CHIS/0001

The Head of Service shall issue the relevant URN to Investigating Officers. This URN shall identify the particular operation and should be cross referenced on associated review, renewal and cancellation forms. Please note that where more than one application is required within any particular investigation, each application shall have its own URN.

Rejected forms will also have their own URN's.

The cross-referencing of each URN takes place within the various forms for audit purposes.

#### Section 1 – Rank and Position of the Authorising Officer

- Please note that the exact position of the Authorising Officer should be given.

#### Section 2 – The Purpose of the operation or investigation

- Include what you want to do and why;
- Include details of the investigation and enquiries to date;
- State your objectives of the operation, i.e. what you seek to achieve by using a CHIS, which should fit in with what you are asking to be authorised.

#### Section 3 – The purpose for which the CHIS (source) will be tasked or deployed

- Explain how their use relates to the investigation in progress.
- Is their purpose to provide information that they already have, i.e. act as an informant) or will it be to build a relationship or get actively involve with certain people, organisations, activities etc. i.e. go undercover etc.?

#### Section 4 – What will the CHIS (source) be tasked to do or how will they be deployed

- Include details of the CHIS, including whether they are vulnerable or juvenile.
- Include details of exactly what they will be required to do.

**Remember that you can only do what you are authorised to do so you need to be as thorough and as detailed as possible in this section.**

## Section 5 – The grounds on which the conduct or use of a CHIS (source) is necessary

This will always be for the purpose of preventing or detecting crime or detecting disorder, in respect of specific offences. Other grounds are not available to local authorities.

## Section 6 – Why the conduct or use of a CHIS (Source) is necessary this particular case

- State that you suspect a criminal offence is being committed, what it is, and if known, what legislation you suspect it is being committed under.
- Also include reasons why it is necessary to use a CHIS, for example: -
  - Other methods of evidence/intelligence gathering have been tried and failed;
  - Overt enquiries will lead to the subject knowing of the investigation and hamper the evidence gathering process;
  - Only way to identify the perpetrator etc.

## Section 7 – Where a specific investigation or operation is involved, details of that investigation or operation

- Describe in as much detail as possible the investigation or operation being undertaken.

## Section 8 – Provide details of any potential collateral intrusion, why the intrusion is unavoidable and precautions that will be taken to minimise collateral intrusion

- Describe how contact is made with the CHIS and where.
- There will be collateral intrusion on neighbours, family members, members of the public, other employees, other customers etc.
- State why the collateral intrusion is unavoidable, e.g. it is the only location available to meet the CHIS, etc.
- Details of how the collateral intrusion will be kept to a minimum, e.g. by using sufficiently trained staff to achieve the objectives, managing the interaction carefully with the CHIS thereby reducing/minimizing collateral intrusion, the need for the CHIS will cease once the objectives are achieved etc.
- All information will be recorded and retained in accordance with DPA and CPIA principles.

## Section 9 – Explain why the conduct or use of a CHIS (source) is proportionate to what it seeks to achieve

Are you asking to do a lot to achieve a little? DO NOT use a sledgehammer to crack a nut!! In considering the proportionality, you should consider the following (this list is not exhaustive):

-

- Serious nature of offence;
- Prevalence of type of offence;
- Impact on victims;
- If not authorised offences may continue without the required evidence to prosecute the offender;
- The use of the CHIS will ultimately lead to prosecution of offender;
- Insufficient evidence to prosecute;
- Deterrent effect of prosecution on perpetrator and wider public;
- Our responsibility to the public and environment etc.;
- Our responsibility to the public purse?
- What is the cost of the criminal activity to the Council and ultimately the public? Specify figures where available.
- Community safety;
- Crime rate;
- Economy of local area;
- Other methods of evidence/intelligence gathering have been tried and failed;
- Overt enquiries will lead to the subject knowing of the investigation and hamper the evidence gathering process;
- May reduce additional collateral intrusion by shortening the length of the investigation;
- Consequences of not taking any action are.....;

Please note that where you want to use a vulnerable or juvenile CHIS you will need to make sure that you explain why it is proportionate to use them.

Please note that it will never be acceptable or justifiable for a juvenile CHIS to provide information about their parents or legal guardians.

## Section 10 – Confidential Information

- Identify how likely, and if so, what type of confidential information may be acquired as a result of using the CHIS.

## Section 11 – Applicants details

This is self-explanatory

Section 12 onwards must be completed by the Authorising Officer.

Before taking the form to the Authorising Officer, the Investigating Officer must take the form completed up to and including Section 11 back to the RIPA Coordinator, for them to satisfy themselves that it is completed correctly and can now be taken to the Authorising Officer.

Once the RIPA Coordinator is satisfied, they will give the partially completed form back to the Investigating Officer who will then take it to the Authorising Officer, who will then follow the next part of the process as set out below.

## **Applications for authorisation for use of a CHIS – Authorisation procedures for Authorising Officers**

For the avoidance of doubt, only those officers authorised under Fenland District Council's Constitution to be 'Authorising Officers' for the purpose of RIPA can authorise the use and/or conduct of a CHIS.

Responsibility for authorising the use and/or conduct of a CHIS rests with the Authorising Officer. The Regulation of Investigatory Powers (Directed Surveillance and Covert Human Intelligence Sources) Order 2010 designates the required level of office for each Authorising Officer.

An Authorising Officer must give authorisations in writing, except that in urgent cases they may be given orally by the Authorising Officer or in writing by the officer entitled to act in urgent cases. In such cases, a record that the Authorising Officer has expressly authorised the action should be recorded in writing by both the Authorising Officer and the applicant as soon as is reasonably practicable, together with the information detailed below.

In addition, they must have received appropriate training. If an Authorising Officer has not received appropriate training, they CANNOT carry out or approve/reject any action set out in this Corporate Policy & Procedures Document.

Authorising Officers **must exercise their minds every time they are asked to sign a form.** They must never sign or rubber stamp Form(s) without thinking about their personal and Fenland District Council's responsibilities.

Finally, an Authorising Officer should not authorise the conduct/use of a CHIS where they are directly involved in the investigation for which it is required. Accordingly, authority should be provided by an alternative Authorising Officer (it does not matter if they are from a



different service). It is not acceptable to use “copy and paste” from previous forms; each application must be individually and carefully considered.

## Section 12 – Authorising Officer – Necessity and Proportionality

You need to state in your own words why you believe the use or conduct of a CHIS is necessary (i.e. justify that it is for the prevention/detection of crime and disorder) and why you believe it to be proportionate to what is being sought by carrying it out.

## Section 13 – Confidential Information Authorisation

If there is a likelihood of acquiring confidential information you should supply detail that demonstrates compliance with the Codes of Practice.

## Date of first Review/Programme for Subsequent Reviews

The Authorising Officer must set a date for review of the authorisation and review on that date; please see notes on reviews below.

## **Approval by a justice of the peace (JP)**

Once the use of a CHIS has been authorised as detailed above, the Authorising Officer will pass the completed authorisation to the RIPA Coordinator for consideration, acting as an independent check at that time.

The Coordinating Officer **must** contact the Court to apply for approval from a JP using the prescribed form shown at [Annex B](#) of this report. In addition [Annex A](#) shows a flowchart of the application process.

They will need to arrange a hearing for the application to be heard, which the Authorising Officer will attend with:-

- RIPA authorisation form signed by an Authorising Officer,
- The accompanying Judicial application form,
- All other relevant documents (sufficient supporting information that will allow the JP to make a fully informed decision).

At the hearing the JP will:-

- Refuse to grant the surveillance, in which case the process must stop and the Council seek fresh approval internally and at Court with more detailed information,
- Grant approval to undertake the surveillance.

## After approval by a JP

The directed surveillance can take place as authorised subject to the time restrictions placed on it. When it expires, it must be renewed by completing the full application process above including gaining approval from a JP.

### Section 17 – Urgent Authorisation

**Urgent applications must still be made to a Justice of the Peace after authorisation. See Annex B for this process.**

## Urgent oral authorisations

These **are not** permitted under any circumstances.

## Duration

The 'authorisation' to use a CHIS is only valid for twelve months from the date on which a Justice of the Peace has approved the authorised RIPA application (from 00:01 on the date on which a Justice of the Peace has approved the authorised RIPA application to 23:59 on the day that is the last day of the twelve months starting from the first day of this period) for the use of CHIS.

A written authorisation will, unless renewed, cease to have effect at the end of a period of twelve months beginning with the day on which it took effect, except for authorisations concerning juveniles, whereby the authorisation will last only one month.

## Reviews

Regular reviews of authorisations should be undertaken to assess the need for the use of a CHIS to continue. Furthermore, any change in circumstances will prompt the need for a review.

There is a standard form available for this purpose on the Home Office website [www.homeoffice.gov.uk](http://www.homeoffice.gov.uk) and on the intranet.

The Investigating Officer should complete the form and submit to the Authorising Officer in time for it to be signed on the date specified on the original application or previous review. The sections are similar to that on the original authorisation form and accordingly the same principles should be applied. In addition, the review should include the use made of the CHIS during the period authorised, the tasks given to the CHIS and the information obtained from the CHIS.

The Authorising Officer shall determine how often a review should take place, however, there shall be no more than one month between the grant of the application and the first

review and one month between subsequent reviews, and not more than one week where the CHIS is a juvenile. More frequent reviews should take place where the use of a CHIS provides access to confidential information or involves collateral intrusion, or uses a vulnerable CHIS.

The results of the review must be recorded on the central record of authorisations and on the Service's own record of authorisations.

## Renewals

As with the initial application, renewals must be approved by a Justice of the Peace before they can be acted upon.

An authorisation can be renewed before it ceases to have effect if an Authorising Officer considers it necessary and proportionate for the use or conduct of a CHIS to continue. The renewal takes effect at the time at which the authorisation would have ceased to have effect. If necessary a renewal can be made more than once. A written renewal may authorise the use or conduct of a CHIS for a further 12 months, or one month in the case of a juvenile CHIS.

Before an Authorising Officer renews an authorisation, he must be satisfied that frequent reviews have been carried out of the use of a CHIS as outlined above.

The Authorisation Officer must consider the matter afresh but also take into account the use made of the CHIS during the period authorised, the tasks given to the CHIS and the information obtained from the CHIS and any collateral intrusion that has occurred.

Renewals should be made in writing on the appropriate form; there is a standard form available for this purpose on the Home Office website [www.homeoffice.gov.uk](http://www.homeoffice.gov.uk) and on the intranet.

Renewal forms should be completed and submitted for authorisation up to 3 days prior to the expiry of the proposed surveillance activity and **no longer**. Any longer than this and it is likely that the circumstances set out in the form will have changed and any authorisation will be out of date.

If there is any deviation from the above, Investigating Officers must check and ensure that the circumstances of the investigation have not changed before obtaining authorisation for a renewal. Where there has been a change in circumstances the application for renewal will need to be revised before being submitted to the Authorising Officer.

A renewal must be recorded on the central record of authorisations and on the service's own record of authorisations.

**A renewal MUST be submitted for approval by a Justice of the Peace before it can be put into operation.**

## **Cancellations**

The Authorising Officer who granted or renewed the authorisation must cancel it if the grounds for granting the authorisation no longer apply, i.e. the aims have been met or the risks/circumstances have changed and the current authorisation is no longer appropriate.

There is a standard form available for this purpose from the Legal team. Once completed these forms must be kept on the central record of authorisations and on the service's own record of authorisations. The Authorising Officer must inform those involved that the use or conduct of the CHIS is no longer required and any activities must cease.

Where necessary, the safety and welfare of the CHIS should continue to be taken into account after the authorisation has been cancelled. The cancellation does not need to be advised or approved by a Justice of the Peace.

## **Records of all CHIS**

Proper records must be kept of the authorisation and use of a source, including details of the CHIS. Certain particulars must be included in the records relating to each CHIS. These are contained in the Regulation of Investigatory Powers (Source Records) Regulations 2000, which are appended to this document.

These records should be maintained in such a way as to preserve the confidentiality of the CHIS and the information provided by that CHIS. The relevant head of service will have responsibility for maintaining these records.

## **Retention and destruction of the product**

Any material which is obtained in the course of a criminal investigation and which may be relevant to the investigation must be recorded and retained. This includes not only material that supports the prosecution's case, but that which may cast doubt on it or supports the defence's case.

- All material that may be relevant to the investigation must be kept until a decision has been taken whether to institute proceedings.
- If proceedings are instituted, all material that may be relevant must be kept until either the accused is acquitted or convicted or the prosecution decides not to proceed with the case.
- Where the accused is prosecuted, all material that may be relevant must be retained until, in the case of a custodial sentence being imposed, the convicted person is released from custody or the expiry of six months, whichever is the longer period, or six months from the date of conviction in all other cases.

- Where an appeal is in progress that material must be kept until the conclusion of the appeal.

Authorising Officers must also ensure compliance with the appropriate Data Protection requirements and any relevant codes of practice produced by the authority in the handling and storage of material. Please refer to the Councils Data Protection Policy.

The head of service shall be responsible for handling, storage and destruction of material obtained through directed surveillance. Please note that material that is obtained, particularly evidence, shall be stored securely both for data protection purposes and to avoid any accusation of tampering with evidence. Material obtained from properly authorised directed surveillance can be used in other investigations.

## Management of CHIS

The Council must ensure proper oversight and management of the CHIS by appointing Officers with these roles in respect of the CHIS:-

1. Handler,
2. Controller,
3. Record Keeper

The following paragraphs explain the purpose and responsibilities of these roles in more detail.

The “Handler” will have day to day responsibility for: -

- Dealing with the CHIS on behalf of the authority concerned;
- Directing the day to day activities of the CHIS;
- Recording the information supplied by the CHIS; and
- Monitoring the CHIS’s security and welfare.

The “Handler” should be below the rank and position of an Authorising Officer and cannot be the Investigating Officer.

The “Controller” will have the responsibility of overseeing the activities of the Handler and should be an Officer of the Council with a higher rank than the Handler and this should be the Service Manager for the Service in which the authorisation is being sought in respect of.

The “Record Keeper” is the Officer with responsibility for maintaining a record of the use made of CHIS. This will normally be the Head of Service responsible for the service using the CHIS.

Officers should consult the RIPA Coordinator for further advice.

# CHIS

## Procedure Checklist

The basic procedure for obtaining authorisation for the Use or Conduct of a CHIS is as follows: -

- The Investigating Officer should undertake a full risk assessment of use of the CHIS before starting this process including considering how any data obtained from them will be held and recorded securely.
- The Investigating Officer having considered the aim of the operation, the health and safety of the CHIS (Including carrying out a risk assessment), the requirements of necessity, proportionality and collateral intrusion (including carrying out a risk assessment) shall complete the application form.
- They shall then seek agreement from the RIPA Coordinator to proceed, and then submit the form to the Authorising Officer (no more than 3 days prior to the anticipated commencement of the operation).
- The Authorising Officer shall consider the requirements of necessity, proportionality and collateral intrusion and if satisfied shall authorise the form for a duration appropriate to the individual circumstances of the case (but not more than 12 months) noting that the authorisation will apply from the date and time on which a Justice of the Peace approves the authorisation.
- The Authorising Officer shall provide a copy of the application whether rejected or authorised to the Investigating Officer and to the RIPA Coordinator for a final check, who will also place a copy on the central file.
- If satisfied the RIPA Coordinator will liaise with the Court to arrange for the Authorising Officer to attend Court to seek approval for surveillance to commence.
- The Authorising Officer will make an application to a Justice of the Peace using the form at Annex B of this policy. Only once the Justice of the Peace gives approval, can the matter proceed.
- In order to make the required application to a Justice of the Peace, the Investigations Officer must be properly authorised to do so under section 223 of the Local Government Act 1972.
- At the time of authorisation the Authorising Officer shall set a date for a review (not more than 1 month from the date of the authorisation, more frequent where required).
- The Investigating Officer shall commence the operation once authorised.
- Not more than 3 days prior to the date for review (and where there has been a change of circumstances) the Investigating Officer shall complete and submit the review form to the Authorising Officer.

- If satisfied that the operation is still necessary and proportionate, the Authorising Officer shall sign off the review form and set a further date for review.
- The Authorising Officer shall provide a copy of the review whether rejected or authorised to the Investigating Officer and the Head of Service and send the original to the Monitoring Officer (central file).
- If, when the Authorisation is near expiry of the, a renewal is deemed necessary, the Investigating Officer shall complete the renewal form, and in doing so shall carry out the same considerations as for the initial application, and additionally include the value of the operation to date.
- They shall submit the renewal form to the Authorising Officer not more than 3 days prior to the expiry of the previous authorisation.
- The Authorising Officer shall consider the requirements of necessity, proportionality and collateral intrusion and if satisfied shall authorise the form for a duration appropriate to the individual circumstances of the case (but not more than 12 months).
- At this point the Investigating Officer must again make an application to a Justice of the Peace using the form at Annex B of this policy. Only once the Justice of the Peace gives approval, can the matter proceed.
- The Authorising Officer shall provide a copy of the renewal form whether rejected or authorised to the Investigating Officer and the Head of Service and send the original to the Monitoring Officer (central file).
- At the time of the authorisation the Authorising Officer shall set a date for a review (not more than 1 month from the date of the authorisation, less if necessary) and carry on as previously.
- Once the operation is complete or the authorised time period has expired the Investigating Officer shall complete a cancellation form which they shall submit to the Authorising Officer.
- The Authorising Officer shall provide a copy of the cancellation form to the Investigating Officer and the Head of Service and send the original to the Monitoring Officer (central file).
- Where necessary the Investigating Officer shall continue to monitor the health and safety of the CHIS after the operation has finished.

# **Part 3**

## **Acquisition of Communications Data**



# Acquisition of Communications Data

## Definition

### What is communications data?

The term 'communications data' embraces the 'who', 'when' and 'where' of a communication but not the content, either said or written. It includes the manner in which, and by what method, a person or machine communicates with another person or machine. It excludes what they say or what data they pass on within that communication.

The Regulation of Investigatory Powers (Communications Data) Order 2004 only permits local authorities to gain access to two types of communications data: service use information and subscriber information.

- **Service use information,**

This is data relating to the use made by any person of a postal or telecommunications service, or any part of it.

Examples of data within this definition include: -

- Itemised telephone records (numbers called);
- Itemised records of connections to internet services;
- Itemised timing and duration of service usage (calls and/or connections);
- Information about amounts of data downloaded and/or uploaded;
- Information about provision of conference calling, call messaging, call waiting and call barring telecommunication services;
- Information about selection of preferential numbers or discount calls;
- Records of posted items, such as records of registered, recorded or special delivery postal items, records of parcel consignments, delivery and collection.

- **Subscriber information**

This is information held or obtained by a Communications Service Provider (CSP) about persons to whom the CSP provides or has provided a communications service.

Examples of data within this definition include: -

- Subscriber checks, reverse look ups etc. such as "who is the subscriber of phone number 01234 567890?", "who is the account holder of e-mail account [xyz@xyz.com](mailto:xyz@xyz.com)?" and "who is entitled to post to web space [www.xyz.abcd.co.uk](http://www.xyz.abcd.co.uk)?";

- Subscribers or account holders account information, including payment method(s) and any services to which the account holder is allocated or has subscribed;
- Addresses for installation and billing;

**Investigating officers can request both historical and future information.**

Local authorities are NOT authorised to obtain access to traffic data.

# Acquisition of Communications Data Authorisation Process

## General

The acquisition of communications data can only be lawfully carried out if properly authorised, and in strict accordance with the terms of the authorisation/notice.

For an authorisation to acquire communications data to be granted the Authorising Officer must be satisfied that the request for that information is:-

- In accordance with the law;
- Necessary; and
- Proportionate.

Accordingly, Investigating Officers who will be submitting the application form and Authorising Officers must be familiar with the following information.

**All authorised applications must also be approved by a Justice of the Peace in addition to by the Authorising Officer. Further action in accordance with RIPA can only take place with the approval of a Justice of the Peace.**

## In accordance with the law

RIPA provides a statutory mechanism that makes certain interference with a person's private life in accordance with the law, including, the acquisition of communications data.

The only data that a Local Authority can properly acquire is subscriber information or service use information. Any request outside this remit will not be in accordance with the law.

## Necessary

An authority may be granted that by an Authorising Officer if they believe that the acquisition of communications data is necessary on the grounds of **preventing or detecting crime or of preventing disorder**. None of the other grounds specified in RIPA are available to local authorities.

Accordingly, it will only ever be necessary to acquire communications data where it is suspected that a crime is being committed.

## Proportionate

If the acquisition of communications information is necessary for the prevention or detection of crime or disorder the Authorising Officer must then go on to consider whether or not it is proportionate. This involves balancing the extent of the intrusiveness of the interference

with an individual's right to respect for their private life against a specific benefit to the investigation or operation being undertaken.

In considering proportionality, the Authorising Officer should consider the following:

- The means should not be excessive by relation to the gravity of the mischief being investigated.
- The least intrusive means of acquiring that information should be chosen. Please note that it cannot be proportionate if there is reasonably available an overt means of finding out the information desired.
- Take into account the risk of intrusion into the privacy of persons other than the specified subjects of investigation: 'collateral intrusion' (see below). Measures must be taken wherever practicable to avoid or minimise so far as is possible collateral intrusion.
- Special consideration should be given where any activity is likely to result in the acquisition of confidential material.

## **Collateral intrusion**

Collateral intrusion is where there is a risk of intrusion into the privacy of persons other than those who are directly the subjects of the investigation or operation.

The Authorising Officer must consider the risk of collateral intrusion and whether a separate authorisation is required for any collateral intrusion or interference with the privacy of persons other than the subject(s) of the investigation.

The person carrying out the investigation must inform the Authorising Officer if the investigation or operation unexpectedly interferes with the privacy of individuals not covered by the authorisation. The Authorising Officer must then review the existing authorisation.

## **General rules**

Acquisition of communications data involves three separate roles:-

- The Applicant /Investigating Officer.
- The Authorising Officer.
- The Single Point of Contact (SPoC).

The SPoC is an accredited individual trained to facilitate the lawful acquisition of communications data and effective co-operation between a public authority and communication service provider (CSP). The legislation requires that for any authority to acquire communications data in accordance with RIPA it must have an accredited SPoC. For a list of accredited SPoC's at Fenland District Council please see [Annex 1](#).

There are two ways in which communications data may be obtained, firstly by way of an authorisation to allow Fenland District Council to collect the communications data itself, and secondly by way of a service of a notice upon the holder of communications data to provide

the information specified in the notice. The service of a notice will be the more common of the two powers utilised to obtain communication data. On the basis that a CSP will have far greater means to obtain the information on Fenland District Council's behalf, only the procedure relating to this process is included in this policy document. If you think you may require an authorisation to acquire that information yourself from the CSP, you should contact the Monitoring Officer who will assist you in that process.

## Forms

The application form, notice, application for cancellation, notice of cancellation and SPoC rejection forms are available from the Legal team.

Only these approved RIPA forms should be used. Any other forms used will be rejected by the Authorising Officer/SPoC.

## Information to be provided in applications for communications data - Investigating Officers

### SPoC Reference Number

This is the reference number provided by the SPoC.

### Application Reference Number

The Investigating Officer should insert his own file reference number in here.

### Unique Reference Number (URN)

Each application form will have a Unique Reference Number (URN) as follows: -

*Year/Service\*/Type of authorisation\*\*/Number\*\*\**

2006/F/CD/0001

\*The services are as follows: -

Environmental Protection (EP), Environmental Health (EH), Environmental Services (ES), Planning (P), Housing (H), Fraud (F), Anti-Social Behaviour (ASB,) Building Control (BC), Internal Audit (IA)

\*\*Communications Data (CD)

(Please note that this is here for identification purposes only and will have no bearing on the numbering.)

\*\*\*Each service shall start at 0001 and run consecutively irrespective of the type of authorisation.

The Head of Service shall issue the relevant URN to Investigating Officers. This URN shall identify the particular operation and should be cross referenced on associated review, renewal and cancellation forms. Please note that where more than one application is required within any particular investigation, each application shall have its own URN.

Rejected forms will also have their own URN's.

The cross-referencing of each URN takes place within the various forms for audit purposes. Name, Service, Rank/Grade (position) and telephone number of the Applicant (Investigating Officer)

- This is self-explanatory.

#### Section 2 – Provide the grounds under which the data is necessary

This will **always** be for the purpose of preventing or detecting crime or detecting disorder; the others are not available to local authorities.

#### Section 3 – Provide details of the Nature of the Enquiry/intelligence Case

- Details of the investigation and enquiries to date;
- Specify what you want to do and why;
- State how accessing the data will further the enquiry;
- Where relevant give the exact time/date/place of the incident under investigation;
- Include relevant subject details – name, DoB, address, their role in the enquiry/investigation

#### Section 4 – Provide details of service/data required

Subscriber information: -

- State telephone number(s) you require subscriber/account information on.
- If not requesting information on most current subscriber, please provide date/time period to search.

OR

Outgoing call data/itemised billing: -

- State telephone number, subscriber details and date/time period from and to

(Please note that subscriber information must have been obtained prior to this request.)

**You cannot request both subscriber information and outgoing/itemised billing in the same application.**

#### Section 5 – Outline the Source of the numbers/other data in the application

- State how the numbers/information were identified, discovered etc...

Section 6 – Explain the reasons why accessing the communications data is necessary on the ground specified

- State that you suspect a criminal offence is being committed, what it is, and if known, what legislation you suspect it is being committed under.
- Also include reasons why it is necessary to access the communications data, for example: -
  - Other methods of evidence/intelligence gathering have been tried and failed;
  - Overt enquiries will lead to the subject knowing of the investigation and hamper the evidence gathering process;
  - Only way to identify the perpetrator etc.

Section 7 – Explain the reasons why the acquisition of the communications data is considered proportionate to what it seeks to achieve

Ensure the objectives have been identified and how obtaining the data will achieve the objectives. Explain why the objectives cannot reasonably be achieved by less intrusive means.

Are you asking to do a lot to achieve a little? DO NOT use a sledgehammer to crack a nut!! In considering the proportionality, you should consider the following (this list is not exhaustive):

-

- Serious nature of offence;
- Prevalence of type of offence;
- Impact on victims;
- If not authorised offences may continue without the required evidence to prosecute the offender;
- Acquisition of data will ultimately lead to prosecution of offender;
- Insufficient evidence to prosecute
- Deterrent effect of prosecution on perpetrator and wider public;
- Our responsibility to the public and environment etc.;
- Our responsibility to the public purse?
- What is the cost of the criminal activity to the Council and ultimately the public? Specify figures where available.

- Community safety;
- Crime rate;
- Economy of local area;
- Other methods of evidence/intelligence gathering have been tried and failed;
- Overt enquiries will lead to the subject knowing of the investigation and hamper the evidence gathering process;
- May reduce additional collateral intrusion by shortening the length of the investigation;
- Consequences of not taking any action are.....;

Section 8 – Provide details of any potential collateral intrusion, why the intrusion is unavoidable and precautions that will be taken to minimise collateral intrusion

- Describe the scene, and where necessary attach a plan or a map etc...
- There will be collateral intrusion on other phone users/joint account holders including family members, members of the public, other employees, other customers etc.
- State why the collateral intrusion is unavoidable, e.g. it is the only means of identifying the identity of the suspected perpetrator etc., the methods used are the only available options etc.
- Details of how the collateral intrusion will be kept to a minimum, e.g. by using sufficiently trained staff to achieve the objectives, by focusing the data requested on the designated subject with set objectives thereby reducing/minimizing collateral intrusion, the acquisition of data will cease once the objectives are achieved etc., the acquisition of data only be used for the evidence and intelligence gathering purposes and will focus on the subject/activity taking place etc.
- All information will be recorded and retained in accordance with DPA and CPIA principles.

Applicant

The investigation officer shall sign and date the form before forwarding it to an accredited SPoC for consideration.

## **Assessing the application form for acquisition of communications data – authorising officers**

For the avoidance of doubt, only those officers authorised under this policy to be an 'Authorising Officer' for the purpose of RIPA can authorise the acquisition and disclosure of



communications data. The Regulation of Investigatory Powers (Communications Data) Order 2010 designates the required level of office for each Authorising Officer.

The prescribed office is described as Director; Head of Service; Service Manager; or equivalent.

Additionally, they must have received appropriate training. If an Authorising Officer has not received appropriate training, they CANNOT approve/reject any action set out in this Corporate Policy & Procedures Document and sign forms.

Authorising Officer should not authorise directed surveillance where they are actively involved in the investigation for which it is required. Accordingly, authority should be provided by an alternative Authorising Officer (it does not matter if they are from a different service).

Authorising Officers **must exercise their minds every time they are asked to sign a form**. They must never sign or rubber stamp Form(s) without thinking about their personal and Fenland District Council's responsibilities.

You must be satisfied that the acquisition of data is necessary and proportionate, and that any potential collateral instruction has been appropriately considered. There are no sections on the application form or the Notice for the Authorising Officer to complete as there are with the forms in respect of directed surveillance or use or conduct of a CHIS, however the Authorising Officer should provide written reasons as to why they believe the acquisition of communications data is necessary (i.e. justify that it is for the prevention/detection of crime and disorder) and why you believe it to be proportionate to what is being sought by carrying it out. These written considerations should be attached to the application form.

## **Approval by a justice of the peace (JP)**

Once Surveillance has been authorised as detailed above, the Investigating Officer must contact the Court to apply for approval from a JP using the prescribed form shown at Annex B of this report. In addition Annex A shows a flowchart of the application process.

They will need to arrange a hearing for the application to be heard, and attend it with:-

- RIPA authorisation form signed by an Authorising Officer,
- The accompanying Judicial application form,
- All other relevant documents (sufficient supporting information that will allow the JP to make a fully informed decision).

At the hearing the JP will:-

- Refuse to grant the surveillance, in which case the process must stop and the Council seek fresh approval internally and at Court with more detailed information,
- Grant approval to undertake the surveillance.

## **After approval by a JP**

The directed surveillance can take place as authorised subject to the time restrictions placed on it. When it expires, it must be renewed by completing the full application process above including gaining approval from a JP.

## **Duration of notices**

The notice is only valid for one month from the date on the notice. This means that the notice must be served within that month.

All notice must relate to the acquisition or disclosure of data for a specific date or period and any period should be clearly indicated on the notice. The start and end date should be given, and where a precise start and end time are relevant these must be specified. Where not date is specified it should be take to be the date on the on which the notice was given.

Where a notice relates to the acquisition or obtaining specific data that will or may be generated in the future, the future period is restricted to no more than one month.

In short, where you are seeking historical data there is no limit on the period which you specify in the notice; however the notice must be served on the CSP within one month. Where you are seeking future data, the period for which you can request that data is restricted to one month.

## **Renewal of notices**

Any valid notice may be renewed for a period of up to one month by the service of a further notice. A renewed notice takes effect upon the expiry of the notice it is renewing.

Renewal may be appropriate where there is a continuing requirement to acquire or obtain data that will or may be generated in the future.

The procedure for renewal is as if a fresh application is being made, and accordingly the procedure as set out above should be followed, save for the fact that the SPoC reference, their file reference and the URN shall be the same as the initial application and both the Investigating Officer and Authorising Officer must consider the value of acquiring the communications data to date and why it is necessary and proportionate to continue to obtain that data.

Investigating officers shall mark the top of the application form 'renewal' when completing and submitting the application form, and the SPoC shall mark the top of the notice 'renewal'.

Copies of these documents must be kept on the investigators own file, the service's own file and the originals sent to the Monitoring Officer to be kept on the Central File.

**A renewal MUST be submitted for approval by a Justice of the Peace before it can be put into operation.**

## Cancellations

The Authorising Officer who granted or last renewed a notice must cancel the notice if after granting the notice the grounds for granting the notice no longer apply, i.e. the aims have been met or the risks/circumstances have changed and the current notice is no longer appropriate.

There is a standard application for cancellation form available from the Legal team. Once completed these forms must be kept on the central record of authorisations and on the service's own record of authorisations.

The cancellation does not need to be advised or approved by a Justice of the Peace.

## Retention and destruction of the product

Any material which is obtained in the course of a criminal investigation and which may be relevant to the investigation must be recorded and retained. This includes not only material that supports the prosecution's case, but that which may cast doubt on it or supports the defence's case.

- All material that may be relevant to the investigation must be kept until a decision has been taken whether to institute proceedings.
  - If proceedings are instituted all material that may be relevant must be kept until either the accused is acquitted or convicted or the prosecution decides not to proceed with the case.
  - Where the accused is prosecuted all material that may be relevant must be retained until, in the case of a custodial sentence being imposed, the convicted person is released from custody or the expiry of six months, whichever is the longer period, or six months from the date of conviction in all other cases.
  - Where an appeal is in progress that material must be kept until the conclusion of the appeal.

Be aware that any information obtained as a result of these powers is likely to be 'personal data' within the meaning of the Data Protection Act 1998. Therefore the requirements of the Data Protection Act 1998 and its principles must be adhered to in respect of this data. Please refer to the Council's Data Protection Policy.

The head of service shall be responsible for handling, storage and destruction of material obtained through the acquisition of communications data and shall ensure that any data that is obtained, particularly evidence, shall be stored securely both for data protection purposes and to avoid any accusation of tampering with evidence.

Properly authorised and acquired Communications Data can be used in other investigations.

**Please note that urgent oral authorisations are not permitted for the purposes of this policy.**

# Acquisition of Communications Data

## Procedure Checklist

The basic procedure for requiring a CSP to disclose to us information they already have in their possession or to obtain information which is not already in their possession is as follows.

- The Investigating Officer, having considered the requirements of necessity, proportionality and collateral intrusion, shall complete the application form.
- They shall then submit the application form to the SPoC.
- If the SPoC is satisfied that the application has been made out properly and it is reasonably practicable to obtain the communications data as requested, the SPoC shall complete the relevant sections of the Notice and forward it and the application form to an Authorising Officer for consideration.
- If the SPoC is not satisfied that the application has been made out he shall complete a SPoC rejection form and return copies of both that and the application form to the Investigating Officer. He shall send the originals to the Monitoring Officer for retention on the Central File.
- The Authorising Officer shall consider the application in light of the requirements of necessity; proportionality and collateral intrusion and either authorise or reject the application.
- If authorised, the Authorising Officer shall complete the necessary sections of the Notice including providing the duration of the Notice (not more than one month).
- The Investigating Officer will make an application to a Justice of the Peace using the form at Annex B of this policy. Only once the Justice of the Peace gives approval, can the matter proceed.
- In order to make the required application to a Justice of the Peace, the Investigations Officer must be properly authorised to do so under section 223 of the Local Government Act 1972.
- Once completed the Authorising Officer shall return a copy of the Notice to the SPoC who shall serve it on the CSP.
- If rejected, he shall provide written reasons why and return a copy of the notice to the SPoC.
- Whether approved or rejected the Authorising Officer shall provide copies of the forms to the Investigating Officer and Head of Service and the originals to the Monitoring Officer (central file).

- When the data is provided by the CSP the SPoC shall feed it back to the Investigating Officer.
- If a renewal is required, it can be renewed for a period of up to one month by following the same procedure as outlined above.
- At this point the Investigating Officer must again make an application to a Justice of the Peace using the form at Annex B of this policy. Only once the Justice of the Peace gives approval, can the matter proceed.
- Once the operation is complete or the time authorised time period has expired the Investigating Officer shall complete a cancellation form which they shall submit to the Authorising Officer for completion.
- The Authorising Officer can either forward the application to cancel to the SPoC who shall draft and serve the Cancellation of Notice on the CSP or draft and serve the Cancellation Notice him/herself.
- The SPoC /Authorising Officer shall send copies of the forms to the Investigating Officer, Head of Service and the Monitoring Officer (central file).

# **Part 4**

## **General Information**

# Collaborative working

In cases where one agency or force is acting on behalf of another, the tasking agency should normally obtain or provide the *authorisation* under Part II of the 2000 Act. For example, where surveillance is carried out by Fenland District Council on behalf of the Police, *authorisations* would usually be sought by the Police and granted by their appropriate *Authorising Officer*. Where the operational support of other agencies (in this example, Fenland District Council) is foreseen, this should be specified in the *authorisation*.

Where possible, *public authorities* should seek to avoid duplication of *authorisations* as part of a single investigation or operation. For example, where two agencies such as Fenland District Council and the Department for Work & Pensions are conducting directed surveillance as part of a joint operation, only one *authorisation* is required. Duplication of *authorisations* does not affect the lawfulness of the activities to be conducted, but may create an unnecessary administrative burden on authorities.

**If in doubt, please consult the Monitoring Officer at the earliest opportunity.**

# Record management

Fenland District Council shall keep detailed records of all authorisations, reviews, renewals, cancellations and rejections within individual services **and** in a central register which shall be maintained and monitored by the Monitoring Officer.

## Records maintained within individual services

Each officer shall keep all of the relevant documents and information relating to the surveillance, use or conduct of CHIS or acquisition of communications data on the case file, including any of the information listed below. In addition, he shall keep details and results of surveillance carried out, information and evidence obtained, etc.

Furthermore, the head of each service shall be responsible for maintaining a register, which shall include all of the following documents/information:-

- Application forms and any supporting documents, including any applications which are rejected;
- Review forms and any supporting information, including details and results of surveillance, conduct or use of CHIS to date;
- Renewal forms and any supporting information, including details and results of surveillance, conduct or use of CHIS to date; including applications which are rejected;
- Cancellation forms and any supporting documents, including an overview of the period over which the surveillance or conduct of use of a CHIS actually took place and value of that.

The register shall be kept in numerical URN order and the head of service shall make regular checks of matters to ensure that the processes are being appropriately followed. Within each URN record, there shall at the very least be an application form (where rejected). Where an application is authorised there will *always* then be a cancellation form and depending on the length of authorisation, a number of review forms. In addition there may be renewal forms.

## Central register maintained by the monitoring officer

Authorising Officers shall forward the original of each of the forms (application whether authorised or rejected, review, renewal, cancellation, notices and rejections) to the Legal Services Manager for the Central Register within 1 week of the authorisation, review, renewal, cancellation or rejection. Please ensure that when sending copies of these forms to the Legal Services Manager they are sent in **sealed** envelopes and marked '**Strictly Private & Confidential**'.

These records shall be retained for a period of at least three years from the ending of the authorisation. The Office of the Surveillance Commissioners (OSC) can audit/review Fenland



District Council's policies and procedures, and individual authorisations and should be made available upon request.

The Monitoring Officer and **RIPA Coordinating Officer** will monitor the forms and give appropriate guidance, from time to time

## **Retention and destruction of the product**

In accordance with the Criminal Procedures and Investigations Act 1996 any material which is obtained in the course of a criminal investigation and which may be relevant to the investigation must be recorded and retained. This includes not only material that supports the prosecution's case, but that which may cast doubt on it or supports the defence's case.

- All material that may be relevant to the investigation must be kept until a decision has been taken whether to institute proceedings.
- If proceedings are instituted, all material that may be relevant must be kept until either the accused is acquitted or convicted or the prosecution decides not to proceed with the case.
- Where the accused is prosecuted, all material that may be relevant must be retained until, in the case of a custodial sentence being imposed, the convicted person is released from custody or the expiry of six months, whichever is the longer period, or six months from the date of conviction in all other cases.
- Where an appeal is in progress that material must be kept until the conclusion of the appeal.

Authorising Officers must also ensure compliance with the appropriate Data Protection requirements and any relevant codes of practice produced by the authority in the handling and storage of material. Please refer to the Council's Data Protection Policy.

The head of service shall be responsible for handling, storage and destruction of material obtained through directed surveillance, conduct of CHIS or acquisition of communications data. Please note that material that is obtained, particularly evidence, shall be stored securely both for data protection purposes and to avoid any accusation of tampering with evidence.

Material obtained from properly authorised directed surveillance can be used in other investigations.

# Member oversight

It is important that Elected Members have oversight of the activity undertaken by Fenland District Council under the RIPA scheme.

On an annual basis the Corporate Governance Committee will review the policy and if necessary make recommendations to full Council for its amendment. In addition Officers will give regular updates during each year on the use of RIPA.

Elected Members are not involved in making decisions on individual authorisations, but are involved taking an overview of types of cases where the powers are used. This oversight is to ensure that the overall balance between the rights of members of the public to privacy and the legitimate needs of the authority to infringe this are kept on the right lines.

# Complaints

Any person who reasonably believes that they have been adversely affected by any activities carried out pursuant to this policy or on behalf of the Council may complain through the Council's complaint procedure. Such a person may also complain to the Investigatory Powers Tribunal. Detail of the relevant complaints procedure can be obtained from the following address: -

The Investigatory Powers Tribunal  
PO Box 33220  
London  
SW1H 9ZQ

Or they can telephone 020 7035 3711.

Further information about the Investigatory Powers Commission is also available at their website:-

<http://www.ipt-uk.com/default.asp>

# Glossary

*Application* A request made to an *Authorising Officer* to consider granting (or renewing) an *authorisation* for directed or intrusive surveillance (under the 2000 Act), or interference with property or wireless telegraphy (under the 1994 or 1997 Act). An *application* will be made by a *member* of a relevant *public authority*.

*Authorisation* An *application* which has received the approval of an *Authorising Officer*. An *authorisation* must comprise a written *application* that has been signed by the *Authorising Officer*.

*Authorising Officer* A person within a *public authority* who is entitled to grant *authorisations* under the 2000 Act or to apply to the *Secretary of State* for such *warrants*. Should be taken to include *senior Authorising Officers*.

*Confidential information* Confidential personal information (such as medical records or spiritual counselling), confidential journalistic material, confidential discussions between *Members* of Parliament and their constituents, or matters subject to *legal privilege*. See Chapter 4 for a full explanation.

*Legal privilege* Matters subject to *legal privilege* are defined in section 98 of the 1997 Act. This includes certain communications between professional legal advisers and their clients or persons representing the client.

*Public authority* Any public organisation, agency or police force (including the military police forces).

*Private information* Any information relating to a person in relation to which that person has or may have a reasonable expectation of privacy. This includes information relating to a person's private, family or professional affairs. *Private information* includes information about any person, not just the subject(s) of an investigation.

*Member* An employee of an organisation, or a person seconded to that organisation (for example, under the terms of section 24 of the Police Act 1996).

*Officer* An *officer* of a police force, HMRC or the OFT, or Officer of a Local Authority or a person seconded to one of these agencies as an *officer*.

*Secretary of State* Any *Secretary of State* (in practice this will generally be the Home Secretary).

# Appendix 1 – List of Authorising Officers and RIPA roles

| Senior Responsible Officer |   |
|----------------------------|---|
| Carol Pilson               | Corporate Director and Monitoring Officer |

| RIPA Coordinator |                              |
|------------------|------------------------------|
| Anna Goodall     | Head of Governance and Legal |

| For all authorisations involving the acquisition of Confidential Material |  |
|---|--|
| Paul Medd   | Chief Executive  |
| Carol Pilson  | Corporate Director and Monitoring Officer<br>(only in cases where Paul Medd is absent) |
| Authorising Officers  |  |
| Paul Medd   | Chief Executive  |
| Brendan Arnold  | Corporate Director and Chief Finance Officer   |
| Richard Cassidy   | Corporate Director   |
| Carol Pilson  | Corporate Director and Monitoring Officer  |
| Geoff Kent  | Head of Customer Services  |

| Single Point of Contact (SPOC) |                               |
|--------------------------------|-------------------------------|
| Kathy Woodward                 | Shared Internal Audit Manager |

The table below explains the different RIPA roles in the Council:-

| <b>The different RIPA roles in the Council</b> |   |
|--|---|
| Senior Responsible Officer                     | <p>This is someone, of at least the rank of authorising officer, responsible for:</p> <ul style="list-style-type: none"> <li>• the integrity of the process in place within the public authority for the management of CHIS and Directed Surveillance;</li> <li>• compliance with Part 2 of the Act and Codes;</li> <li>• engagement with the OSC inspectors when they conduct their inspections, where applicable; and</li> <li>• where necessary, oversight of the implementation of post-inspection action plans approved by the relevant oversight Commissioner.</li> </ul> <p>They are a member of the Council's corporate leadership team and responsible for ensuring that all authorising officers are of an appropriate standard in the light of any recommendations in ICPO inspection reports.</p> |
| RIPA Coordinator                               | <p>A senior officer of the Council who ensures that RIPA is being used correctly, maintains the central record of authorisations and is also independent of the application and authorisation process. A RIPA Co-ordinating Officer (RCO) will be at the heart of day to day management of RIPA, with the SRO as the officer with overall responsibility. They are responsible for:-</p> <ul style="list-style-type: none"> <li>• Maintenance of a Central Record of Authorisations and collation of all original RIPA documentation;</li> <li>• Day to day oversight of the RIPA process, particularly of the submitted documentation;</li> <li>• Organising corporate training for RIPA;</li> <li>• Raising RIPA awareness within the Council.</li> </ul>   |
| Authorising Officer                            | <p>A named Officer authorised by the Council's RIPA policy to scrutinise and authorise (or not) applications to use RIPA that are received from Investigating Officers.</p>   |
| Investigating Officer                          | <p>The Officer requesting the use of RIPA and the one undertaking the work associated with this.</p>  |
| Single Point of Contact or "SPoC"              | <p>The single point of contact (SPoC) is an individual trained to facilitate lawful acquisition of communications data and effective co-operation between a public authority and communications providers.</p>  |
| CHIS Handler                                   | <p>An Officer below the grade of an Authorising Officer who is responsible for day to day contact with the CHIS.</p>  |
| CHIS Controller                                | <p>An Officer who supervises the CHIS Handler.</p>  |

## Appendix 2 — Risk Assessment – collateral intrusion

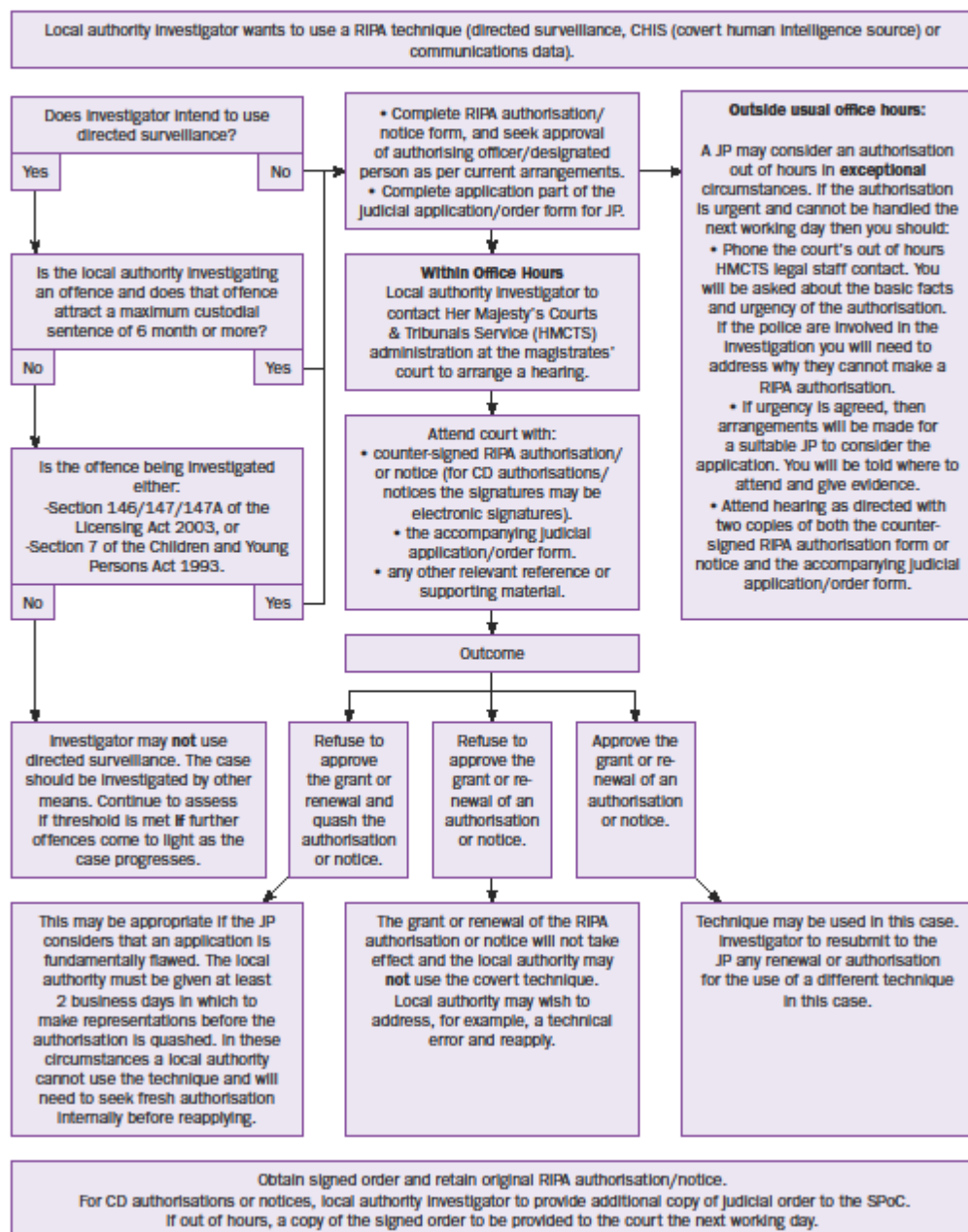
|                                | DETAILS / COMMENTS |
|--------------------------------|--------------------|
| <b><u>Subject Location</u></b> |                    |
| Type of property               |                    |
| Entrance/ exits                |                    |
| Vehicle access                 |                    |
| Public transport               |                    |
| <b><u>Locality</u></b>         |                    |
| Description of area            |                    |
| Type of road, cul-de-sac etc.  |                    |
| Neighbours                     |                    |
| Other buildings                |                    |
| Shops                          |                    |
| Schools                        |                    |
| Lighting                       |                    |
| Sensitivities                  |                    |
| Other                          |                    |
| <b><u>People</u></b>           |                    |
| Family                         |                    |
| Other occupants                |                    |

|   |  |
|---|--|
| Neighbours                                |  |
| Visitors                                  |  |
| Members of the Public                     |  |
| Other                                     |  |
| <b><u>Risk</u></b>                        |  |
| Sensitivities                             |  |
| Confidential information                  |  |
| Informant                                 |  |
| Exposure of operation                     |  |
| Exposure of observation point             |  |
| Health and Safety (staff and public)      |  |
| Equipment                                 |  |
| Disclosure                                |  |
| Communications                            |  |
| Other                                     |  |
| <b><u>Reduction of Risk/Intrusion</u></b> |  |
| Use Intelligence                          |  |
| Correct use of camera/technical equipment |  |
| Other                                     |  |



## ANNEX A

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



ANNEX B

**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 JP:.....

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