	AGENDA ITEM NO. 11
COUNCIL	
Date	**20 DECEMBER 2012**
Title	**REGULATION OF INVESTIGATORY POWERS ACT (RIPA)**

1. PURPOSE/SUMMARY

The Protection of Freedoms Act 2012 has changed how Councils can use the Regulation of Investigatory Powers Act 2000 (RIPA). This means that the Council's RIPA Policy must be updated to take account of this change.

2. KEY ISSUES

- RIPA allows Councils to carry out certain types of surveillance (when investigating suspected benefit fraud, for example). Evidence from these may be used by the Council in court proceedings. The Act details how surveillance must be requested, authorised and conducted.

- The Protection of Freedoms Act 2012 has now taken effect. This fundamentally changes how Councils can use RIPA. This change means Council will have to approve a revised RIPA Policy.

- This report explains the changes required to the Policy.

3. RECOMMENDATIONS

It is recommended that Council:-

- Note this report, and
- Agree the revised Policy to take immediate effect.

Wards Affected	All
Forward Plan Reference No.	RIPA changes to be agreed at Council are in the Plan.
Portfolio Holder(s)	Councillor John Clark, Portfolio Holder for Quality Organisation
Report Originator	Geoff Kent, Head of Customer Services Email: gkent@fenland.gov.uk Tel: 01354 622290

Contact Officer(s)	Alan Pain, Corporate Director and Monitoring Officer Email: alanpain@fenland.gov.uk Rob Bridge, Corporate Director and Chief Finance Officer Email: robbridge@fenland.gov.uk Ian Hunt, Chief Solicitor Email: ihunt@fenland.gov.uk Geoff Kent, Head of Customer Services Email: gkent@fenland.gov.uk
Background Paper(s)	Protection of Freedoms Act 2012 – changes to provisions under the Regulation of Investigatory Powers Act 2000 (RIPA) – Home Office Guidance to local authorities on the judicial approval process for RIPA and the crime threshold for directed surveillance. Home Office, October 2012.

1. INTRODUCTION

1.1 RIPA allows Councils to undertake covert surveillance that can lead to gaining private information about individuals. Such surveillance is lawful if the actions are:-

1. Necessary for the purpose of preventing or detecting crime or preventing disorder,

2. Proportionate. This involves balancing the effect on an individual's human rights of the surveillance with the benefit of the surveillance itself,

3. Non-discriminatory, and

4. Lawful.

2. THE PROTECTION OF FREEDOMS ACT 2012 AND ITS EFFECT ON RIPA

2.1 The above act become law in October 2012.It is designed to safeguard civil liberties and reduce the burden of Government intrusion into the private life of individual citizens.

2.2 Amongst other non-related measures, the Protection of Freedoms Act (Called "the Act" from this point onwards in this report) makes fundamental changes to how local authorities are now able to use RIPA.

2.3 Until the above Act took effect, the way the Council used RIPA was as below:-

1. The need to use directed surveillance was identified. Typically this is where evidence needed to be gathered in relation to suspected serious benefit fraud.

2. The Investigating Officer asks an Authorising Officer (see section 2.4) for approval.

3. If approval was granted, surveillance could take place but only in the exact manner and for the tightly defined period shown on the form.

2.4 The Council Officers designated as "Authorising Officer" are:-

Senior Responsible Officer	
Alan Pain	Corporate Director and Monitoring Officer
For all authorisations involving the acquisition of confidential material	
Paul Medd	Chief Executive
Alan Pain	Corporate Director and Monitoring Officer
Authorised Officers	
Paul Medd	Chief Executive
Alan Pain	Corporate Director and Monitoring Officer
Rob Bridge	Corporate Director and Chief Finance Officer
Richard Cassidy	Corporate Director
Geoff Kent	Head of Customer Services
Single Point of Contact (SPOC)	
Jonathan Tully	Internal Audit
James Brewer	Benefit Fraud
Debbie Chaplin	Benefit Fraud

2.5 Once the Act came into force the process changed in two significant ways:-

1. RIPA authorisations made by Councils must now be approved by a Justice of the Peace.

2. Directed surveillance can only be used where Councils investigate certain types of criminal offence, which must attract a maximum custodial sentence of six months or more, or relate to the underage sale of alcohol or tobacco.

2.6 The effect of the new restrictions in Section 2.5 above is that the Council can only therefore use RIPA to investigate in more serious cases such as serious criminal damage, dangerous waste dumping, serious or serial benefit fraud, preventing or detecting the underage sale of alcohol or tobacco.

2.7 The Council will not be able to use RIPA to investigate what the Home Office calls “low level offences” which include littering, dog control or fly-posting.

2.8 However it is worth noting that the Council has not used RIPA at all for some time.

2.9 Councils can now only use RIPA using three covert techniques, subject to the above constraints:-

1. Directed surveillance – covert surveillance,

2. Covert human intelligence source (CHIS) – undercover officers, informants and people who make test purchases,

3. Communications data – obtaining service use and subscriber information for telephone and internet services (to identify the person involved; it does not include intercepting actual calls or internet traffic itself).

2.10 Some current RIPA arrangements still remain unchanged:-

1. Authorising Officers have to be Director, Head of Service, Service manager or equivalent. The table in 2.4 above shows that we continue to

meet this standard.

2. Time limits for authorisations remain three months, or twelve months for a CHIS. After this time they must be renewed if still needed.

2.11 The Act makes it clear that Councils can only now use RIPA in respect of the strictly specified criteria detailed in section 2.5 (2). Councils cannot use it to investigate disorder that does not involve criminal offences or to investigate low-level offences such as littering, dog control and fly-posting.

2.12 At first glance, these changes will have a major impact on how the Council investigates offences as is slows the investigation process and adds an additional step to it, which could delay obtaining key information (such as the daily routine of a person being investigated for serious benefit fraud, where surveillance can prove if they are going to work each day when claiming they are unemployed).

2.13 In reality, the impact will be minimal as RIPA is rarely used. This is due to the use of a number of other ways to build cases for potential prosecution as well as by working directly with potential offenders to prevent criminal behaviour.

2.14 The procedure for gaining approval to use RIPA has now become:-

1. The need to use RIPA is identified. This must meet the test outlined in section 2.5 (2).

2. The Investigating Officer asks an Authorising Officer for approval.

3. Approval can be given, but action cannot take place without the new and further steps detailed below.

4. The Court (in practice this will be the Magistrate's Court at either Huntingdon or Peterborough) must be contacted to arrange a hearing to hear the application. A copy of the authorisation and supporting documents will be provided to the Court.

5. A hearing will be convened, in private and heard by a single Justice of the Peace (JP). The Council will decide which Officers are designated to attend this type of hearing (the Home Office suggests that legally trained personnel are not needed to present at these hearings).

6. The JP will consider the application and its reasonableness with regards the Act and then approve it (or not). This will be recorded formally with paper copies of the decision form kept by the Council and Court.

7. If approval was granted, surveillance could take place but only in the exact manner and for the tightly defined period shown on the form.

2.15 There is currently no indication that the approval of the RIPA surveillance will attract the charging of fees by the Court.

3.16 The revised Corporate RIPA Policy is attached to this report. The document is marked to indicate where it has been amended and all changes are shown in red.

4. CONCLUSION AND RECOMMENDATION

4.1 Members are asked to:-

1. Note changes to the Council's RIPA Policy required as a result of the Protection of Freedoms Act 2012 on the use of RIPA.

3. Approve the revised policy as attached to this report.

THIS PAGE IS INTENTIONALLY BLANK

FENLAND DISTRICT COUNCIL

CORPORATE POLICY & PROCEDURES

ON

THE REGULATION OF INVESTIGATORY POWERS ACT 2000 (RIPA)

CONTENTS

Introduction		3
DIRECTED SURVEILLANCE		
Surveillance – Definition		6
Authorisation Procedures - Directed Surveillance		11
Authorisation Forms		14
Procedure Checklist – Directed Surveillance		~~23~~24
COVERT HUMAN INTELLIGENCE SOURCE (CHIS)		
Conduct and Use of a Covert Human Intelligence Source (CHIS) - Definition		26
Authorisation Procedures – CHIS		~~27~~28
Procedure Checklist - CHIS		~~38~~39
ACQUISITION OF COMMUNICATIONS DATA		
Acquisition of Communications Data - Definition		41
Authorisation Procedures - Acquisition of Communications Data		~~43~~44
Procedure Checklist – Acquisition of Communications Data		~~51~~53
Collaborative working		~~53~~56
Record Management - General		~~54~~57
Members oversight		~~56~~59
Complaints		~~57~~60
Glossary		~~58~~61
Appendix 1	List of Authorised Posts/Officers	59
Appendix 2	Risk Assessment	60
~~Appendix 3~~	~~Process Flowchart~~	~~62~~
Annex A	Home Office flowchart for RIPA process	67
Annex B	Approval form for use by Justice of the Peace	68

NB:
The Regulation of Investigatory Powers Act 2000 ('RIPA') refers to 'Designated Officers'. For ease of understanding and application within Fenland District Council (FDC), this Corporate Policy & Procedures Document refers to 'Authorised Officers'. For the avoidance of doubt, therefore, all references to duly certified Authorised Officers refer to 'Designated Officers' under RIPA.

VERSION NOTES
This version created 1/12/12 to reflect changes contained in Protection of Freedoms Act 2012. Please note therefore that all reference to the Regulation of Investigatory Powers Act 2000 ("RIPA") should also made in conjunction with the 2012 Act.

Formatted: Left

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 FDC) can interfere with this right, provided it has a good reason and follows the proper procedures. Accordingly, FDC 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. 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 FDC are covered by the Act for the time they are working for FDC. All external agencies must, therefore, comply with RIPA and the work carried out by agencies on FDC's behalf must be properly authorised by one of FDC's designated Authorised Officers. Authorised 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,~~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 FDC 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 Authorised 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.

Formatted: Font: Bold

Formatted: Font: Bold, Underline

Formatted: Font: Bold

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 Regulation of Investigatory Powers (Covert Surveillance and Property Interference: Code of Practice) Order 2010.

The Regulation of Investigatory Powers (Covert Human Intelligence Sources: Code of Practice) Order 2010.

The Regulation of Investigatory Powers (Directed Surveillance and covert Human Intelligence Sources) Order 2010

The Regulation of Investigatory Powers (Directed Surveillance and covert Human Intelligence Sources) (Amendment) Order 2012

Copies of both codes are held within Legal Services or visit:- http://security.homeoffice.gov.uk/ripa/publication-search/general-publications/ripa-cop/index.html

Further useful guidance is available in the publication Office of Surveillance Commissioners Procedures and Guidance - December 2008 (available via the LACORS website) http://www.lacors.gov.uk/lacors/ContentDetails.aspx?authCode=1C80888&id=20820

The Home Office produced guidance on changes to RIPA as a result of the Protection of Freedoms Act 2012:- http://www.homeoffice.gov.uk/publications/counter-terrorism/ripa-forms/local-authority-ripa-guidance/

Formatted: Default, Right: 0 cm

DIRECTED SURVEILLANCE

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 FDC 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 ~~activites~~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 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.

~~Be aware that upon continuing to survey a suspicious event, written or urgent oral authorisation should be sought as soon as is practicable. There is no definitive guide as to how long one can survey before authorisation is sought, however, anything longer than initial observations are likely to require authorisation.~~

Formatted: Indent: Left: 1.06 cm

For what purpose can we conduct Directed Surveillance?

An *authorisation* for directed surveillance by FDC 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. For any Local Authority, these grounds are:

- *F~~ f~~or the purpose of preventing or detecting crime or of preventing ~~disorde~~disorder.*

Formatted: Left

In addition Article 2 of the Regulation of Investigatory Powers (Directed Surveillance and Covert Human Intelligence Sources) (Amendment) Order 2012 inserts a new Article 7A into the Regulation of Investigatory Powers (Directed Surveillance and Covert Human Intelligence Sources) Order 2010 requiring that:
~~r, and~~

- *~~That t~~The local authority is investigating an offence that will attract a maximum custodial sentence of six months or more, or*
- *The offence being investigated is in respect of either Sections 146 /147 /147a of the Licensing Act 2003 or Section 7 of the Children and Young People Act 1993.*

Covert surveillance for any other general purposes should be conducted under other ~~legislation ,~~legislation, if available, and an *authorisation* under Part II of the 2000 Act should not be sought.

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 *officer*s 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**
Overt Not requiring prior authorisation	- Police Officer or Parks Warden on patrol - Signposted Town Centre CCTV cameras (in normal use) - Recording noise coming from outside the premises after the occupier has been warned that this will occur if the noise persists. - Most test purchases (where the officer behaves no differently from a normal member of the public).
Covert Not requiring prior authorisation	- CCTV cameras providing general traffic, crime or public safety information.
Directed Must be RIPA authorised	- Officers follow an individual or individuals over a period, to establish whether s/he is working when claiming benefit or off long term sick from employment. - 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 s/he is suspected of ~~running his business in an unlawful manner~~selling alcohol or tobacco to under-age customers~~.~~. - 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.
Intrusive **FDC cannot do this**	- Planting a listening or other device (bug) in a person's home or in their private vehicle. - Using the public CCTV system to look inside a ~~persons~~person's home, or private vehicle in a planned way.

.

AUTHORISATION PROCEDURE

GENERAL

An authorisation under Part II of the 2000 Act will, providing the statutory tests are met, provide a lawful basis for FDC 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 Authorised 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 the Authorising Officer. Further action in accordance with RIPA can only take place with the approval of a Justice of the Peace.

Formatted: Font: Bold

NECESSITY AND PROPORTIONALITY

Is the surveillance activity *necessary*?

An authority may be granted by an Authorised Officer if s/he believes that the use of directed Surveillance 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 carry out directed surveillance where it is suspected that a crime is being committed.

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 Authorised 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 Authorised 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 Authorised 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 ~~has~~ and Monitoring Officer have 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.

AUTHORISATION FORMS

The authorisation forms are standard forms which are appended to this document and are available on the Home Office website www.homeoffice.gov.uk. Only these approved RIPA forms should be used. Any other forms used will be rejected by the Authorised Officers.

Blank forms are also available on the intranet.

These forms should be completed and submitted for authorisation ~~up to 3 days~~as early as possible prior to the start of the proposed surveillance activity. ~~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.~~ 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 - INFORMATION REQUIRED FROM INVESTIGATING OFFICERS

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 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 Authorised Officer

- Please note that the exact position of the Authorised 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, ~~eg~~e.g. static or foot mobile surveillance;
- What is being surveyed, ~~eg~~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, ~~eg~~e.g. camera, video, CCTV, recording equipment, binoculars ~~etc~~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~~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 the for the purpose of preventing or detecting crime or of preventing disorder; the others are not available to local authorities.

Section 7 – Explain the reasons why the directed surveillance 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 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~~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~~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.

APPLICATION FOR AUTHORISATION FOR DIRECTED SURVEILLANCE - AUTHORISATION PROCEDURES

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

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

For the avoidance of doubt, only those officers authorised under this policy to be 'Authorised Officers' for the purpose of RIPA can authorise directed surveillance. See Appendix 1 – List of Authorised Officers. No other Officers can give approval.

An Authorised Officer must give authorisations in writing, except that in urgent cases they may be given orally by the Authorised Officer or in writing by the officer entitled to act in urgent cases. In such cases, a record that the Authorised Officer has expressly authorised the action should be recorded in writing by both the Authorised 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 Authorised Officer has not received appropriate training, s/he **cannot** approve/reject any action set out in this policy**.**

Authorised 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 FDC's responsibilities.

An Authorised 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 Authorised Officer (it does not matter if they are from a different service).

Section 12 – Authorised 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 – Authorised 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 Authorised 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 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 Authorised 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

~~Urgent oral authorisations should not be necessary. In exceptional circumstances, however, urgent authorisations may be given orally if the time that would elapse before a written authorisation can be granted would be likely to endanger life or jeopardise the investigation or operation for which the authorisation was being given.~~

~~It will not be urgent where the need for authorisation has been neglected or because the Officer has delayed.~~

Formatted: Font: Bold, Underline

Formatted: Bulleted + Level: 1 + Aligned at: 0.63 cm + Tab after: 1.27 cm + Indent at: 1.27 cm

Formatted: Font color: Black, Not Expanded by / Condensed by

Formatted: Font color: Black, Not Expanded by / Condensed by

Formatted: Font color: Black, Not Expanded by / Condensed by

Formatted: Bulleted + Level: 1 + Aligned at: 0.63 cm + Tab after: 1.27 cm + Indent at: 1.27 cm

Formatted: Font color: Black, Not Expanded by / Condensed by

Formatted: Left, Bulleted + Level: 1 + Aligned at: 0.63 cm + Tab after: 1.27 cm + Indent at: 1.27 cm

Formatted: Font: Bold

Formatted: Left, Indent: Left: 1.27 cm

Formatted: Font: Bold, Underline

~~Urgent authorisations last for no more than 72 hours.~~

~~In making an application for an urgent authorisation the Investigating Officer will need to communicate all of the information that is required by the application form to the Authorised Officer and the Authorised Officer will need to go through the same process in terms of assessing the application form. In such cases the Authorised Officer and applicant, where applicable, should also record the following information in writing, as soon as is reasonably practicable (it is not necessary to record further detail):~~

- ~~the reasons why the Authorised Officer considered the case so urgent that an oral instead of a written authorisation was given; and,~~

- ~~Where the officer entitled to act in urgent cases has given written authority, the reasons why it was not reasonably practicable for the application to be considered by the Authorised Officer should also be recorded.~~

~~Where authorisations are granted orally under urgency procedures, a record detailing the actions authorised and the reasons why the urgency procedures were used should be recorded by the applicant and Authorised Officer as a priority. There is then no requirement subsequently to submit a full written application;~~ These are no longer permitted under any circumstances.

DURATION

The 'authorisation' to carry out/conduct the surveillance lasts for a maximum of 3 months (from authorisation) for Directed Surveillance. However, care should be taken not to automatically authorise for the maximum time allowed; each application should be assessed individually. Authorisation should only last as long as is deemed necessary and proportionate.

Urgent oral authorisation, if not already ratified in a written authorisation, will cease to have effect after 72 hours, beginning with the time when the authorisation was granted.

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 on the Home Office website www.homeoffice.gov.uk and on the intranet.

In each case the frequency of reviews should be considered at the outset by the Authorised Officer or, for those subject to authorisation by the Secretary of State, the member or officer who made the application within the public authority concerned. 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 Authorised 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 Authorised Officer by means of a review. The Authorised 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 or intrusive 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 Authorised 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 Authorised 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 on the Home Office website 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 Authorised Officer.

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

In exceptional circumstances, renewals may be granted orally in urgent cases and last for a period of seventy-two hours and a full record of this should be made as soon as is practicable after the oral renewal is made on the renewal form.

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.

Formatted: Font: Bold

CANCELLATIONS

The Authorised 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 on the Home Office website www.homeoffice.gov.uk and on the intranet. Once completed these forms must be kept on the central record of authorisations and on the service's own record of authorisations.

The Authorised 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.

Formatted: Left

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 Authorised 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;
- whether the urgency provisions were used, and if so why;
- if the authorisation has been renewed, when it was renewed and who authorised the renewal, including the name and rank/grade of the Authorised 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 Authorised Officer;
- a record of the period over which the surveillance has taken place;
- the frequency of reviews prescribed by the Authorised 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 *Authorised Officer*.

PROCEDURE CHECK LIST FOR DIRECTED SURVEILLANCE

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 complete the application form.

- S/he shall then submit the form to the Authorised Officer (no more than 3 days prior to the anticipated commencement of the surveillance activity).

- The Authorised 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).

- The Authorised Officer shall provide a copy of the application whether rejected or authorised to the Investigating Officer and the Head of Service and send the original to the Monitoring Officer (central file).

- 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.

- At the time of authorisation the Authorised 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 Authorised Officer.

If satisfied that the surveillance activity is still necessary and proportionate, the Authorised Officer shall sign off the review form and set a further date for review.

- The Authorised 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 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.

- S/he shall submit the renewal form to the Authorised Officer not more than 3 days prior to the expiry of the previous authorisation.

Formatted: List Paragraph, Right: 0 cm, No bullets or numbering, Adjust space between Latin and Asian text, Adjust space between Asian text and numbers

- The Authorised 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 Authorised 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 Authorised 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 s/he shall submit to the Authorised Officer.

Formatted: Indent: Left: 0.63 cm, No bullets or numbering

Formatted: No bullets or numbering

Formatted: Indent: Left: 0.63 cm, No bullets or numbering

COVERT HUMAN INTELLIGENCE SOURCE (CHIS)

CONDUCT AND USE OF A 'COVER HUMAN INTELLIGENCE SOURCE' (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.

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 FDC as part of their normal civic duties, or to contact numbers set up to receive information.

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.

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.

AUTHORISATION PROCEDURE – CHIS

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 Authorised 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 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 be granted by an Authorised Officer if s/he believes that the conduct and use of the CHIS 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.

Proportionality

If the conduct or use of a CHIS is necessary for the prevention or detection of crime or disorder the Authorised Officer must then go on to consider whether or not the proposed use or conduct of a CHIS is proportionate. In considering proportionality, the Authorised 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 of conduct of a CHIS, the Authorised 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 that 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 Authorised 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 Authorised Officer if the investigation or operation unexpectedly interferes with the privacy of individuals not covered by the authorisation. The Authorised Officer must then consider wither 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 Authorised 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 Authorised 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.

Additional Safeguards when Authorising a CHIS

When authorising the conduct or use of a CHIS, an Authorised 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.

AUTHORISATION FORMS

The authorisation forms are standard forms which are appended to this document and are available on the Home Office website www.homeoffice.gov.uk. Only these approved RIPA forms should be used. Any other forms used will be rejected by the Authorised Officers.

These forms are at also available on the intranet.

These forms should be completed and submitted for authorisation up to 3 days prior to the start of the proposed use or conduct of a CHIS and no longer. Any longer that this and it is likely that the circumstances set out in the form will have changed and any authorisation would be out of date.

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.

INFORMATION TO BE PROVIDED IN APPLICATIONS FOR AUTHORISATION

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 Authorised Officer

- Please note that the exact position of the Authorised 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

- E.g. In relation to an organised serious crime, espionage, a series of racially motivated crimes ~~etc~~etc.;
- 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~~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, the other grounds are not available to local authorities.

Section 6 – Why the conduct or use of a CHIS (Source) 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 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 – Details of any potential collateral intrusion, why it is unavoidable and precautions that will be taken to minimise it

- 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 8 – 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;
- 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…..;

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 his/her parents or legal guardians.

Section 9 – Confidential Information

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

Section 10 – Applicants details

This is self-explanatory

ASSESSING THE APPLICATION FORM

For the avoidance of doubt, only those officers authorised under FDC's Constitution to be 'Authorised 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 Authorised Officer. The Regulation of Investigatory Powers (Directed Surveillance and Covert Human Intelligence Sources) Order 2010 designates the required level of office for each Authorised Officer.

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

An Authorised Officer must give authorisations in writing, except that in urgent cases they may be given orally by the Authorised Officer or in writing by the officer entitled to act in urgent cases. In such cases, a record that the Authorised Officer has expressly authorised the action should be recorded in writing by both the Authorised 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 Authorised Officer has not received appropriate training, s/he CANNOT carry out or approve/reject any action set out in this Corporate Policy & Procedures Document.

Authorised 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 FDC's responsibilities or sign any forms.

Finally, an Authorised 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 and alternative Authorised Officer (it does not matter if they are from a different service).

Section 12 – Authorised 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 Authorised 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 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 Authorised 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.

Formatted: No underline
Formatted: Font: Bold
Formatted: No underline
Formatted: No underline
Formatted: No underline
Formatted: No underline
Formatted: Indent: Left: 1.27 cm, No bullets or numbering
Formatted: Font: Bold
Formatted: No underline

Section 17 – Urgent Authorisation

~~**You should explain why you considered the case so urgent that an oral instead of written authorisation was given.**~~

Formatted: Font: Bold

~~**Please note that where the authorisation is oral, the detail referred to above should be recorded in writing by the applicant as soon as reasonably practicable.**~~**Urgent applications must still be made to a Justice of the Peace after authorisation. See Annex B for this process.**

URGENT ORAL AUTHORISATIONS

~~Urgent authorisations should not be necessary. In exceptional circumstances, however, urgent authorisations may be given orally if the time that would elapse before a written authorisation can be granted would be likely to endanger life or jeopardise the investigation or operation for which the authorisation was being given.~~

~~It will not be urgent where the need for authorisation has been neglected or because the Officer has delayed.~~

~~Urgent authorisations last for no more than 72 hours.~~

~~In making an application for an urgent authorisation the investigation officer will need to communicate all of the information that is required in the application form to the Authorised Officer and the Authorised Officer will need to go through the same process in terms of assessing the application as if it were a written application.~~

~~The information must then be recorded in writing on the standard application form as soon as practicable afterwards, but certainly not more than 72 hours from the grant of the urgent authorisation. The extra boxes on the form must be completed to explain why the authorisation was urgent.~~

~~Accordingly, both the Investigating Officer and the Authorised Officer shall make detail contemporaneous notes of the conversation, copies of which shall be attached to the subsequently completed application form.~~

~~They must be recorded in writing on the standard form as soon as practicable and the extra boxes on the form completed to explain why the authorisation was urgent.~~

~~Accordingly, both the Investigating Officer and Authorised Officer shall make detailed contemporaneous notes of the conversation, copies of which shall be attached to the subsequently completed application form.~~

~~A member of the Litigation Team or the Monitoring Officer in The Monitoring Officer can be contacted for advice in the event that and an Authorised Officer is asked to authorise an urgent oral authorisation.~~ These are no longer permitted under any circumstances.

DURATION

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.

However, care should be taken not to automatically authorise for the maximum time allowed; each application should be assessed individually; each application should be assessed on its own facts. Authorisation should only last as long as is deemed necessary and proportionate.

Urgent oral authorisations or authorisations granted or renewed by an Authorised Officer will, unless renewed, cease to have effect after seventy-two hours, beginning with the time when the authorisation was granted or renewed.

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 and on the intranet.

The Investigating Officer should complete the form and submit to the Authorised 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 Authorised 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

An authorisation can be renewed before it ceases to have effect if an Authorised 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 ~~that~~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 Authorised 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 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 Authorised Officer.

In exceptional circumstances, renewals may be granted orally in urgent cases and last for a period of seventy-two hours. A full record should be made as soon as is practicable after the oral renewal is made on the renewal form.

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.

Formatted: Font: Bold

CANCELLATIONS

The Authorised 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 ~~not longer~~no longer appropriate.

There is a standard form available for this purpose on the Home Office website www.homeoffice.gov.uk and on the intranet. Once completed these forms must be kept on the central record of authorisations and on the service's own record of authorisations.

The Authorised 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.

Authorised 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 Investigating Officer 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;

PROCEDURE CHECKLIST FOR USE OR CONDUCT OF A CHIS

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

- 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.
- S/he shall then submit the form to the Authorised Officer (no more than 3 days prior to the anticipated commencement of the operation).
- The Authorised 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).
- The Authorised Officer shall provide a copy of the application whether rejected or authorised to the Investigating Officer and the Head of Service and send the original to the Monitoring Officer (central file).
- 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.
- At the time of authorisation the Authorised 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 Authorised Officer.
- If satisfied that the operation is still necessary and proportionate, the Authorised Officer shall sign off the review form and set a further date for review.
- The Authorised 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.
- S/he shall submit the renewal form to the Authorised Officer not more than 3 days prior to the expiry of the previous authorisation.

Formatted: Indent: Left: 0.63 cm, No bullets or numbering

- The Authorised 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.

Formatted: No bullets or numbering

- The Authorised 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 Authorised 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 s/he shall submit to the Authorised Officer.

- The Authorised 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.

ACQUISITION OF COMMUNICATIONS DATA

ACQUISITION OF COMMUNICATIONS DATA

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?" and "who is entitled to post to web space 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.

AUTHORISATION PROCEDURE – ACQUISITION OF COMMUNICATIONS DATA

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 Authorised 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 Authorised Officers must be familiar with the following information.

All authorised applications must also be approved by a Justice of the Peace IN ADDITION TO 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 Authorised Officer if s/he believes 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 Authorised 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 Authorised 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 Authorised 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 that the subject(s) of the investigation.

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

GENERAL RULES

Acquisition of communications data involves three separate roles: the applicant/Investigating Officer, the Authorised Officer and 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 FDC, please see Appendix 1.

There are two ways in which communications data may be obtained, firstly by way of an authorisation to allow FDC 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 FDC'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 standard forms and are available on the Home Office website www.homeoffice.gov.uk and on the intranet.

You will note that the 'application for communication data' form appended to this document has been amended to coincide with this policy. Accordingly, if an application is made on a form obtained directly from the website, Investigating Officers, SPoC's and Authorised Officers must in any event ensure compliance with this policy. All reference on the home office forms to 'Authorised Officer' is in fact 'Authorised Officer' for the purpose of this policy.

Only these approved RIPA forms should be forms. Any other forms used will be rejected by the Authorised 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, ~~eg~~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, ~~eg~~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 – AUTHORISED OFFICERS

For the avoidance of doubt, only those officers authorised under this policy to be an 'Authorised 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 Authorised Officer.

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

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

Authorised 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 Authorised Officer (it does not matter if they are from a different service).

Authorised 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 FDC'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 Authorised Officer to complete as there are with the forms in respect of directed surveillance or use or conduct of a CHIS, however the Authorised 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 Authorised 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

Formatted: Font: Bold
Formatted: No underline
Formatted: No underline
Formatted: No underline
Formatted: No underline
Formatted: Indent: Left: 1.27 cm, No bullets or numbering
Formatted: Font: Bold
Formatted: No underline

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 Authorised 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.

Formatted: Font: Bold

CANCELLATIONS

The Authorised 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 and standard notice of cancellation available for this purpose on the Home Office website www.homeoffice.gov.uk and on the intranet. 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 ~~case~~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. ~~There fore~~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 Councils 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.

PROCEDURE CHECKLIST FOR ACQUISITION OF COMMUNICATIONS DATA

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.
- S/he 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 Authorised 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 Authorised 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 Authorised 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 Authorised 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 Authorised 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.

Formatted: Indent: Left: 0.63 cm, No bullets or numbering

Formatted: Bullets and Numbering

Formatted: List Paragraph, Right: 0 cm, No bullets or numbering, Adjust space between Latin and Asian text, Adjust space between Asian text and numbers

- Once the operation is complete or the time authorised time period has expired the Investigating Officer shall complete a cancellation form which s/he shall submit to the Authorised Officer for completion.

- The Authorised 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 /Authorised Officer shall send copies of the forms to the Investigating Officer, Head of Service and the Monitoring Officer (central file).

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 FDC on behalf of the Police, *authorisations* would usually be sought by the Police and granted by their appropriate *Authorised Officer*. Where the operational support of other agencies (in this example, FDC) 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 FDC 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

FDC 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

Authorised 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 FDC's policies and procedures, and individual authorisations and should be made available upon request.

The Monitoring Officer and Legal Services Manager and 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.

Authorised 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, 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 FDC 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 ~~to~~ the ~~committee~~ Committee will review the operation of the scheme on a quarterly basis.

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 7273 4514.

GLOSSARY

Application A request made to an *Authorised 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 *Authorised Officer*. Depending on the circumstances, an *authorisation* may comprise a written *application* that has been signed by the *Authorised Officer*, or an oral *application* that has been verbally approved by the *Authorised Officer*.

Authorised Officer A person within a *public authority* who is entitled to grant *authorisations* under the 2000 or 1997 Acts or to apply to the *Secretary of State* for such *warrants*. Should be taken to include *senior Authorised Officers*.

Confidential information Confidential personal information (such as medical records or spiritual counselling), confidential journalistic material, confidential discussions between *Member*s 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 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 AUTHORISED OFFICERS

For all authorisations involving the acquisition of Confidential Material	
~~Sandra Claxton~~Paul Medd	~~Deputy~~ Chief Executive
Alan Pain	Corporate Director and Monitoring Officer

Senior Responsible Officer	
~~Sandra Claxton~~Alan Pain	~~Deputy Chief Executive~~Corporate Director and Monitoring Officer

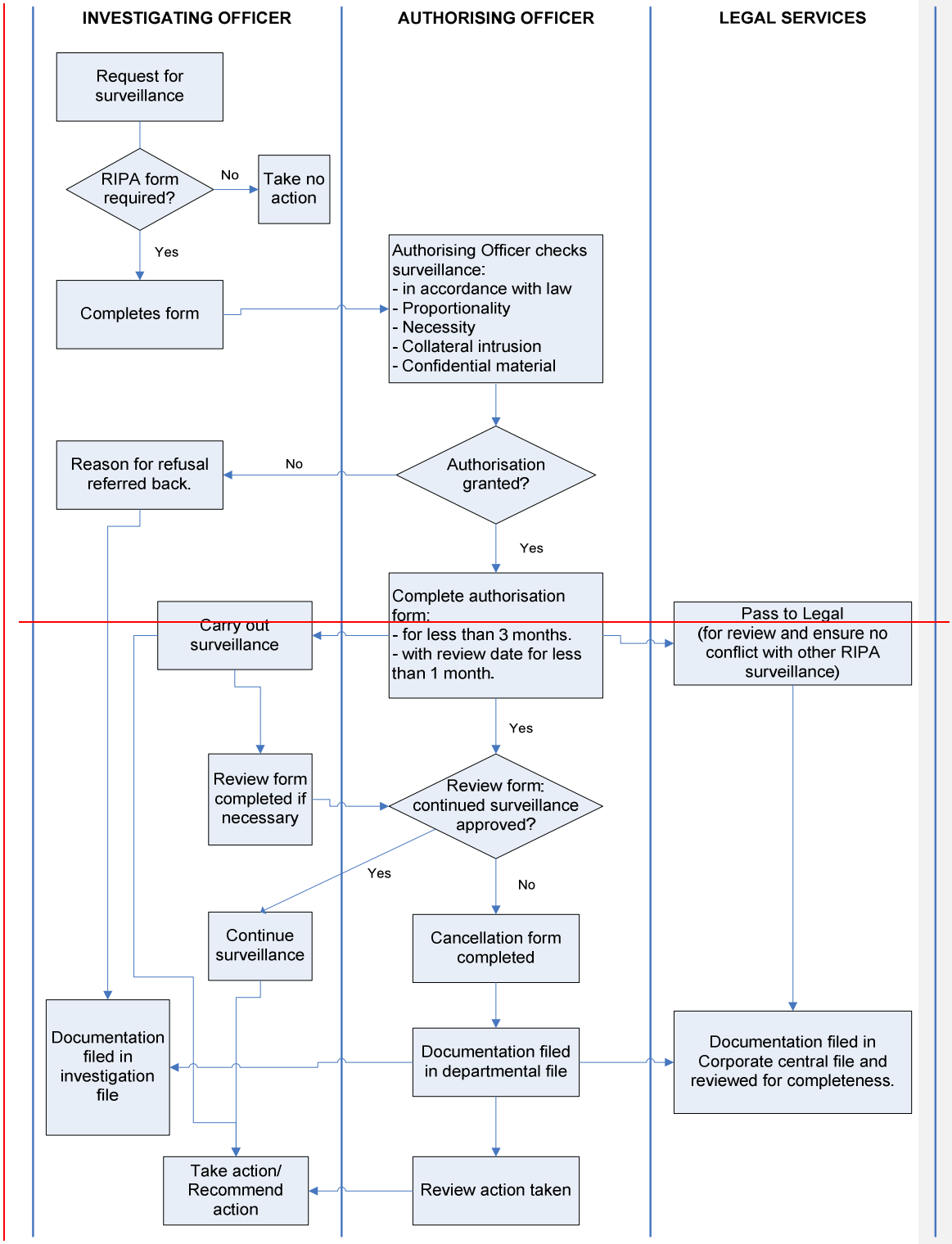
Authorised Officers	
Paul Medd	~~Executive Director~~Chief Executive
Alan Pain	Corporate Director and Monitoring Officer
Rob Bridge	Corporate Director and Chief Finance Officer
Richard Cassidy	Corporate Director
Geoff Kent	Head of ~~Income & ICT~~Customer Services

Single Points of Contact (SPOC)	
~~Carl Holland~~Jonathan Tully	~~Finance Manager for Internal Audit and Corporate Services~~Internal Audit
James Brewer	~~Investigations Officer Income & ICT~~Benefit Fraud
Debbie Chaplin	~~Investigations Officer Income & ICT~~Benefit Fraud

APPENDIX 2 –– RISK ASSESSMENT – COLLATERAL INTRUSION

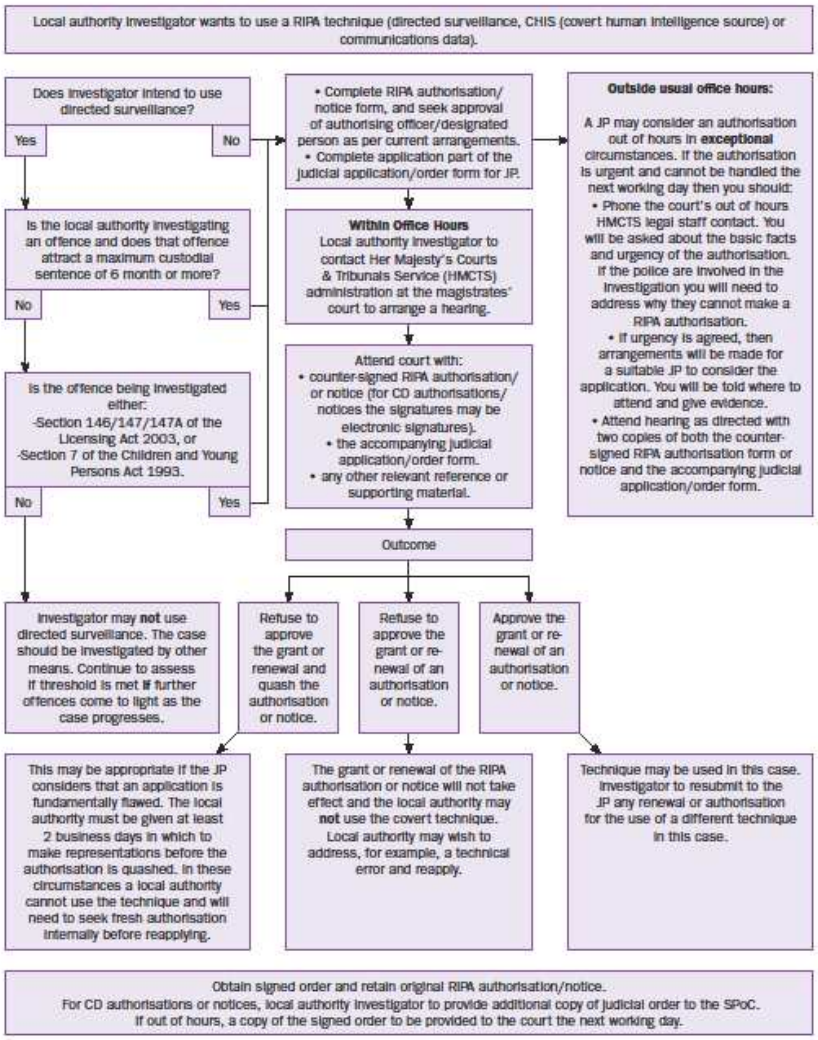
	DETAILS / COMMENTS
Subject Location	
Type of property	
Entrance/ exits	
Vehicle access	
Public transport	
Locality	
Description of area	
Type of road, cul-de-sac etc	
Neighbours	
Other buildings	
Shops	
Schools	
Lighting	
Sensitivities	
Other	
People	
Family	
Other occupants	
Neighbours	
Visitors	
Members of the Public	
Other	

Risk	
Sensitivities	
Confidential information	
Informant	
Exposure of operation	
Exposure of observation point	
Health and Safety (staff and public)	
Equipment	
Disclosure	
Communications	
Other	
Reduction of Risk/Intrusion	
Use Intelligence	
Correct use of camera/technical equipment	
Other	


INVESTIGATING OFFICER
AUTHORISING OFFICER
LEGAL SERVICES
Request for surveillance
RIPA form required?
No
Take no action
Yes
Completes form
Authorising Officer checks surveillance:
- in accordance with law
- Proportionality
- Necessity
- Collateral intrusion
- Confidential material
Authorisation granted?
No
Reason for refusal referred back.
Yes
Complete authorisation form:
- for less than 3 months.
- with review date for less than 1 month.
Carry out surveillance
Pass to Legal
(for review and ensure no conflict with other RIPA surveillance)
Yes
Review form completed if necessary
Review form: continued surveillance approved?
Yes
No
Continue surveillance
Cancellation form completed
Documentation filed in investigation file
Documentation filed in departmental file
Documentation filed in Corporate central file and reviewed for completeness.
Take action/ Recommend action
Review action taken

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



17

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:.....

18

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:

19