## Contents

| A | Corporate Policy Statement | 4 |
| B | Definitions | 5 |
| C | Introduction | 6 |
| D | RIPA | 7 |
| E | Responsibilities of Authorised Officers, the Senior Responsible Officer and Members | 9 |
| F | Types of Surveillance | 10 |
| G | Conduct and Use of a Covert Human Intelligence Source (CHIS) | 13 |
| H | Authorisation Procedures | 15 |
| I | Working With/Through Other Agencies | 20 |
| J | Acquisition and Disclosure of Communications Data | 21 |
| K | Records | 24 |
| L | Complaints | 25 |
| M | Summary | 25 |

- Appendix 1 - List of Authorised Officer Posts | 26
- Appendix 2 - Flowchart | 27
- Appendix 3 - Application to a Justice Of The Peace Seeking an Order to Approve the Grant of a RIPA Authorisation or Notice | 28
- Appendix 4 - Judicial Order | 29
- Appendix 5 - Directed Surveillance Forms | 31
- Appendix 6 - Covert Human Intelligence Sources Forms
- Appendix 7 - Communications Data Forms
A. Corporate Policy Statement

1. The Council takes seriously its statutory responsibilities and will at all times act in accordance with the law and take necessary and proportionate action in these types of matters. In that regard the Council’s Solicitor is duly authorised to keep this document up to date and amend, delete, add or substitute relevant provisions, as necessary.

2. It is this Council’s Policy that:

   • All covert surveillance exercises for the purposes of preventing or detecting crime or of preventing disorder conducted by the Council should comply with the requirements of RIPA

   • Only the Authorised Officers for the Department proposing to undertake covert surveillance are permitted to authorise a covert surveillance operation

   • No Authorised Officer should authorise a covert surveillance operation until he or she has demonstrated that he or she has the competence to do so

   • A CHIS would be used only rarely and in exceptional circumstances

3. The District Council’s Constitution and in particular the provisions of the Scheme of Delegation to Officers empowers the Chief Executive, Director of Corporate Resources, Director of Regeneration & Neighbourhoods and Head of Corporate Services to: grant, review, renew and cancel authorisations under the Regulation of Investigatory Powers Act 2000.
## B. Definitions

<table>
<thead>
<tr>
<th>Term</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>The Policy</td>
<td>Bassetlaw District Council Corporate Policy &amp; Procedure Document on RIPA</td>
</tr>
<tr>
<td>Authorised Officers</td>
<td>RIPA refers to “Designated Officers”. For ease of understanding and application this document refers to Authorised Officers. These are those posts referred to in Appendix 1 and any that are duly added to or substituted by the Senior Responsible Officer. For Authorised Officer’s responsibilities go to section E</td>
</tr>
<tr>
<td>Senior Responsible Officer</td>
<td>The Council’s Solicitor. For details of responsibilities go to section E.</td>
</tr>
<tr>
<td>Central Register</td>
<td>This is kept by the Senior Responsible Officer and will contain copies of RIPA authorisations, authorisations, cancellations and renewals.</td>
</tr>
<tr>
<td>Members</td>
<td>Elected members of Bassetlaw District Council. For Members responsibilities go to Section E.</td>
</tr>
<tr>
<td>SPOC</td>
<td>Home Office accredited Single Point of Contact. For responsibilities go to section J.</td>
</tr>
<tr>
<td>CHIS</td>
<td>Covert Human Intelligence Source. For conduct and use of a CHIS see section G.</td>
</tr>
<tr>
<td>Surveillance Commissioners</td>
<td>The Office of Surveillance Commissioners is the statutory body with powers of inspection of all authorities that have the powers to use covert surveillance. Bassetlaw District Council is regularly inspected.</td>
</tr>
</tbody>
</table>
C. Introduction

This document is based on the requirements of the Regulation of Investigatory Powers Act 2000 (RIPA) and the Home Office’s Code of Practice for Directed Surveillance Covert Human Intelligence Sources (CHIS) and Disclosure of Communications Data and related regulations and orders. It also includes the non-statutory Home Office Guidance to local authorities on the judicial approval process for RIPA and the crime threshold for directed Surveillance issues October 2012.

The authoritative position on RIPA is the Act itself and any Officer who is unsure about any aspect of this document should contact the Senior Responsible Officer for advice and assistance. All Authorised Officers, other senior managers and operational officers who have received appropriate training may apply for an authorisation. Refresher training will be organised as appropriate.

Copies of this document are available on the internet and intranet. The forms are also available on the intranet.

The Senior Responsible Officer will maintain and check the Central Register of all authorisations, reviews, renewals, cancellations and rejections. It is the responsibility of the relevant Authorised Officer to ensure that the Senior Responsible Officer receives the relevant form within 1 week of its completion. The Senior Responsible Officer will routinely check all forms included on the Central Register, including applications and authorisations, to ensure compliance with RIPA and relevant guidance and codes of practice. The Central Register will be used by the Senior Responsible Officer to exercise effective oversight and quality control. Once an authorisation has been given the Senior Responsible Officer will use the Central Register to identify when reviews, renewals and cancellations are due and maintain oversight of compliance with due dates.

RIPA and this document are important to the effective and efficient operation of the Council’s action with regard to the use of covert surveillance and Covert Human Intelligence Sources. This document will be kept under review by Members & the Senior Responsible Officer. Authorised Officers must bring suggestions for continuous improvements to the attention of the Senior Responsible Officer at the earliest opportunity.

In terms of monitoring e-mails and internet usage, it is important to recognise the interplay and overlap with the Council’s e-mail and internet policies and guidance, the Telecommunications (Lawful Business Practice)(Interception of Communications) Regulations 2000, the Data Protection Act 1998 and its related guidance and Codes of Practice. RIPA forms should only be used where relevant and they will only be relevant where the criteria listed on the forms is fully met.

If you are in any doubt on RIPA, this document or the related legislative provisions, please consult the Senior Responsible Officer at the earliest opportunity.

Logs of access to the Internet and use of e-mail are maintained by the Head of Corporate Services. With effect from 5th January 2004 local authorities gained new powers and responsibilities under RIPA to access communications data (for the purpose of preventing or detection of crime or preventing disorder) by virtue of the Regulation of Investigatory Powers (Communications Data) Order 2003 (“the 2003 Order”) which brought into effect the provisions of Chapter II of RIPA. Requests for access to and disclosure of such data will only be able to be made through a designated (in accordance with RIPA and the 2003 Order) Officer who is also a Home Office accredited Single Point of Contact (“SPOC”). The Council will continue to ensure that it has at least one accredited SPOC in place for this purpose.
D. RIPA

1. The Human Rights Act 1998 (which brought much of the European Convention on Human Rights and Fundamental Freedoms 1950 into UK domestic law) requires the District Council, and organisations working on its behalf, pursuant to Article 8 of the European Convention, to respect the private and family life of citizens, their home and their correspondence.

2. The European Convention did not, however, make this an absolute right, but a qualified right. Accordingly, in certain circumstances, the District Council may interfere in the citizen’s right mentioned above, if such interference is:-

   (a) in accordance with the law;
   (b) necessary (as defined in this Document); and
   (c) proportionate (as defined in this Document).

3. 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 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, the RIPA seeks to ensure that both the public interest and the human rights of individuals are suitably balanced.

4. Necessary and proportionate

The Home Office’s Code of Practice provides as follows:

(i) Obtaining an authorisation under RIPA will only ensure that there is a justifiable interference with an individual’s Article 8 rights if it is necessary and proportionate for these activities to take place. RIPA first requires that the person granting an authorisation believes that the authorisation is necessary in the circumstances of the particular case for one or more of the statutory grounds in Section 28(3) of RIPA for directed surveillance”.

(ii) Then, if the activities are necessary, the person granting the authorisation must believe that they are proportionate to what is sought to be achieved by carrying them out. This involves balancing the intrusiveness of the activity on the target and others who might be affected by it against the need for the activity in operational terms. The activity will not be proportionate if it is excessive in the circumstances of the case or if the information which is sought could reasonably be obtained by other less intrusive means. All such activity should be carefully managed to meet the objective in question and must not be arbitrary or unfair.

(iii) Take into account the risk of intrusion into the privacy of persons other than the specified subject of the surveillance (Collateral Intrusion). Measures must be taken wherever practicable to avoid or minimise (as far as possible) collateral intrusion and the matter may be an aspect of determining proportionality.

(iv) Ensuring the perceived crime or offence satisfies the crime threshold for Directed Surveillance.
5. Directly employed Council staff and external agencies working for the District Council are covered by the Act for the time they are working for the District Council. All external agencies must, therefore, comply with RIPA and the work carried out by agencies on the Council’s behalf must be properly authorised by one of the Council’s designated Authorised Officers. Authorised Officers are those posts appearing in Appendix 1 and any that are duly added to or substituted by the Senior Responsible Officer.

6. If the correct procedures are not followed, evidence may be disallowed by the courts, 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 the District Council and will, undoubtedly, be the subject of adverse press and 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 Senior Responsible Officer. A flow chart of the procedures to be followed appears at Appendix 2.

7. What RIPA does and does not do

RIPA does:

• require prior authorisation and judicial approval of directed surveillance
• prohibit the Council from carrying out intrusive surveillance
• require authorisation for the conduct and use of a CHIS
• require safeguards for the conduct and use of a CHIS

RIPA does not:

• make unlawful conduct which is otherwise lawful
• prejudice or disapply any existing powers available to the District Council to obtain information by any means not involving conduct that may be authorised under this Act. For example, it does not affect the District Council’s current powers to obtain information via the DVLA or to get information from the Land Registry as to the ownership of a property.

If the Authorised Officer or any Applicant is in any doubt, s/he should ask the Senior Responsible Officer BEFORE any directed surveillance and/or CHIS is authorised, renewed, cancelled or rejected.
E. Responsibilities of the Senior Responsible Officer, Authorised Officers and Members

1. The Senior Responsible Officer is the Council’s Solicitor. The Senior Responsible Officer is responsible for: the integrity of the process in place to authorisesurveillance and interference with wireless telegraphy; compliance with the Act; engagement with the Surveillance Commissioners and inspectors when they conduct their inspections, and where necessary, overseeing the implementation of any post-inspection action plans recommended or approved by a Surveillance Commissioner.

2. The Senior Responsible Officer will ensure that all Authorising Officers and elected members are made fully aware of and receive copies of this document.

3. It will be the responsibility of Authorised Officers to ensure that relevant members of staff are also suitably trained as Applicants so as to avoid common mistakes appearing on Authorisation forms.

4. Authorised Officers must ensure that staff who report to them follow this document and do not undertake any form of surveillance without first obtaining the relevant authorisation in compliance with this document.

5. Authorised Officers must pay particular attention to Health & Safety issues that may be raised by any proposed surveillance activity. Under no circumstances should an Authorised Officer approve any RIPA form unless, and until they are satisfied that the health and safety of the employee or agent are properly addresses and/or the risks minimised, so far as possible, and proportionate to the surveillance being proposed.

6. Authorised Officers must ensure when sending copies of any forms to the Senior Responsible Officer for inclusion in the Central Register, that they are sent in sealed envelopes and marked **Strictly Private & Confidential**.

7. Authorised Officers must ensure that requests for access to and disclosure of communications data under RIPA and the Regulation of Investigatory Powers (Communication Data) Order 2003, are made through the Council’s accredited SPOC.

8. Members will review the use of RIPA and set the policy at least once a year. They will consider internal reports on the use of the RIPA on a quarterly basis, **where RIPA has been used in the preceding quarter**, to ensure that it is being used consistently with the Policy and that the Policy remains fit for purpose. The Senior Responsible Officer will prepare an annual report which will state the number of authorisations granted and a brief outline of the reasons for the authorisations. The report will go to the Scrutiny Committee. The Scrutiny Committee will review the Policy annually and refer to Council if there are any concerns. Members will not, however, be involved in making decisions on specific authorisations.
F. Types of Surveillance

1. ‘Surveillance’ includes:

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

Surveillance can be overt or covert

2. Overt Surveillance

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

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 entertainment licence is issued subject to conditions, and the licensee is told that officers may visit without notice or identifying themselves to the owner/proprietor to check that the conditions are being met.)

7. 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. (Section 26(9)(a) of RIPA).

RIPA regulates two types of covert surveillance, (Directed Surveillance and Intrusive Surveillance) and the use of CHIS.

8. Directed Surveillance

Directed Surveillance is surveillance which:-

   - is covert; and
   - is not intrusive surveillance (see definition below – the Council must not carry out any intrusive surveillance);
   - is not carried out in an immediate response to events which would otherwise make seeking authorisation under the Act unreasonable, e.g. spotting something suspicious and continuing to observe it; and
   - it is undertaken for the purpose of a specific investigation or operation in a manner likely to obtain private information about an individual (whether or not that person is specifically targeted for purposes of an investigation). (Section 26(10) of RIPA).
Private Information

‘Private information’ in relation to a person includes any information relating to his private and family life, his home and his correspondence. The fact that covert surveillance occurs in a public place or on business premises does not mean that it cannot result in the obtaining of private information about a person. Prolonged surveillance targeted on a single person will undoubtedly result in the obtaining of private information about him/her and others with whom s/he comes into contact, or associates with;

Similarly, although overt town centre CCTV cameras do not normally require authorisation, if the camera is tasked for a specific purpose, which involves prolonged surveillance on a particular person, authorisation will be required. The way a person runs his/her business may also reveal information about his or her private life and the private lives of others.

Confidential Information

Particular care should be taken in cases where the subject of the investigation might reasonably expect a high degree of privacy where confidential information is involved.

‘confidential information’ consists of such matters as legal privilege, confidential personal information or confidential journalistic information. So for example particular care should be given where matters of medical or journalistic confidentiality or legal privilege may be involved.

Where it is likely that through the use of surveillance knowledge of confidential information will be acquired the Authorisation must be given by the Chief Executive or in his absence his nominated Deputy.

In general an application for surveillance which is likely to result in the acquisition of legally privileged information should only be made in exceptional and compelling circumstances. Particular regard should be had to the issue of proportionality. Similar considerations should also be given to authorisations that involve confidential personal information and confidential journalistic material.

‘legally privileged’ information applies to communications between a professional legal adviser and their client or any person representing their client which are made in connection with the giving of legal advice to the client or in contemplation of legal proceedings.

‘confidential personal information’ is information held in confidence relating to the physical or mental health or spiritual counselling concerning an individual (whether living or dead) who can be identified from it. Examples might include consultations between a health professional and a patient.

‘confidential journalistic material’ includes material acquired or created for the purposes of journalism and held subject to an undertaking to hold it in confidence.

For the avoidance of doubt, only those officers designated and certified to be Authorised Officers for the purpose of RIPA can authorise ‘Directed Surveillance’ IF, AND ONLY IF, the RIPA authorisation procedures detailed in this Document, are followed. If an Authorised Officer has not been ‘certified’ for the purposes of RIPA, s/he can NOT carry out or approve/reject any action set out in this document.
9. **Intrusive Surveillance**

This is when it:-

- is covert;
- relates to residential premises or private vehicles; and
- Involves the presence of a person in the premises or in the vehicle or is carried out by a surveillance device in the premises/vehicle. Surveillance equipment mounted outside the premises will not be intrusive, unless the device consistently provides information of the same quality and detail as might be expected if they were in the premises/vehicle.

This form of surveillance can be carried out only by the police and other law enforcement agencies. **Council officers must not carry out intrusive surveillance.**

10. **Examples of different types of Surveillance**

<table>
<thead>
<tr>
<th>Type of Surveillance</th>
<th>Examples</th>
</tr>
</thead>
<tbody>
<tr>
<td>Overt</td>
<td>• Police Officer or Parks Warden on patrol</td>
</tr>
<tr>
<td></td>
<td>• Sign-posted Town Centre CCTV cameras (in normal use)</td>
</tr>
<tr>
<td></td>
<td>• Recording noise coming from outside the premises after the occupier has been warned that this will occur if the noise persists.</td>
</tr>
<tr>
<td></td>
<td>• Most test purchases (where the officer behaves no differently from a normal member of the public).</td>
</tr>
<tr>
<td>Covert but not requiring prior authorisation</td>
<td>• CCTV cameras providing general traffic, crime or public safety information.</td>
</tr>
<tr>
<td>Directed must be RIPA authorised</td>
<td>• 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.</td>
</tr>
<tr>
<td></td>
<td>• Test purchases where the officer has a hidden camera or other recording device to record information that 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.</td>
</tr>
<tr>
<td><strong>Intrusive</strong> – the District Council cannot do this!</td>
<td>• Planting a listening or other device (bug) in a person's home or in their private vehicle.</td>
</tr>
</tbody>
</table>
G. Conduct and Use of a Covert Human Intelligence Source (CHIS)

1. **Who is a CHIS**
   Someone who establishes or maintains a personal or other relationship for the covert purpose of helping the covert use of the relationship to obtain information.

   RIPA does not apply in circumstances where members of the public volunteer information to the District Council as part of their normal civic duties, or to contact numbers set up to receive information.

2. **What must be authorised?**
   The Conduct or Use of a CHIS require prior authorisation.
   - Conduct of a CHIS = 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.
   - Use of a CHIS = Actions inducing, asking or assisting a person to act as a CHIS and the decision to use a CHIS in the first place.

   The Council can use a CHIS IF, AND ONLY IF, RIPA procedures, detailed in this Document are followed.

3. **Confidential Information**
   In cases where through the use or conduct of a source it is likely that knowledge of confidential information will be acquired the deployment of the source is subject to a higher level of authorisation. Such authorisations must be given by the Chief Executive or in his absence his nominated Deputy.

   ‘Confidential information’ consists of such matters as legal privilege, confidential personal information or confidential journalistic information. Further details are provided in Section F above.

4. **Juvenile Sources**
   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. Authorisations for juvenile sources can only be granted by the Chief Executive or in his absence his authorised deputy.

5. **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.

   Authorisations for the use of a vulnerable individual as a source can only be granted by the Chief Executive or in his absence his authorised deputy.
6. Test Purchases
Carrying out test purchases will not (as highlighted above) require the purchaser to establish a relationship with the supplier with the covert purpose of obtaining information and, therefore, the purchaser will not normally be a CHIS. For example, authorisation would not normally be required for test purchases carried out in the ordinary course of business (e.g. walking into a shop and purchasing a product over the counter).

By contrast, developing a relationship with a person in the shop, to obtain information about the seller’s suppliers of an illegal product (e.g. illegally imported products) will require authorisation as a CHIS. Similarly, using mobile hidden recording devices or CCTV cameras to record what is going on in the shop will require authorisation as directed surveillance. A combined authorisation can be given for a CHIS and also directed surveillance.

7. Anti-social behavior activities (e.g. noise, violence, race etc)
Persons who complain about anti-social behaviour, and are asked to keep a diary, will not normally be a CHIS, as they are not required to establish or maintain a relationship for a covert purpose. Recording the level of noise (e.g. the decibel level) will not normally capture private information and, therefore, does not require authorisation.

Recording sound (with a DAT recorder) on private premises could constitute intrusive surveillance, unless it is done overtly. For example, it will be possible to sound record if the noisemaker is warned that this will occur if the level of noise continues.

Placing a stationary or mobile video camera outside a building to record anti-social behaviour on residential estates will require prior authorisation.

Social Networking Sites and Internet Sites
Although social networking and internet sites are easily accessible, if they are going to be used during the course of an investigation, consideration must be given about whether RIPA authorisation should be obtained.

Care must be taken to understand how the social media site being used works. Officers must not be tempted to assume that one service provider is the same as another or that the services provided by a single provider are the same.

Whilst it is the responsibility of an individual to set privacy settings to protect against unsolicited access to their private information on a social networking site, and even though the data may be deemed published and no longer under the control of the author, it is unwise to regard it as ‘open source’ or publicly available; the author has a reasonable expectation of privacy if access controls are applied. Where privacy settings are available but not applied the data may be considered open source and an authorisation is not usually required.

If it is necessary and proportionate for the Council to covertly breach access controls, the minimum requirement is an authorisation for directed surveillance. An authorisation for the use and conduct of a CHIS is necessary if a relationship is established or maintained by the officer (i.e. the activity is more than mere reading of the site’s content). This could occur if an officer covertly asks to become a ‘friend’ of someone on a social networking site.

CHIS authorisation is only required when using an internet trading organisation such as E-Bay or Amazon Marketplace in circumstances when a covert relationship is likely to be formed. The use of disguised purchaser details in a simple, overt, electronic purchase does not require a CHIS authorisation, because no relationship is usually established at this stage.
H. Authorisation Procedures

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

Annex 2 provides a flow chart of process from application consideration to the recording of information.

1. Authorised Officers
   Forms can only be signed by Authorised Officers identified in the Council’s Constitution. Authorised posts are listed in Appendix 1. If a Director or Head of Service wishes to add, delete or substitute a post, s/he must refer such request to the Senior Responsible Officer.

   A higher level of authority is required where:
   i. the Directed Surveillance or the use or conduct of a source is likely to produce ‘confidential information’
   ii. the use or conduct of a source who is a juvenile is proposed.
   iii. the use or conduct of a source who is a vulnerable individual is proposed

   In such cases an Authorisation can only be given by the Chief Executive or in his absence his authorised deputy.

   Authorisations under RIPA are separate from delegated authority to act under the Council’s Scheme of Delegation. RIPA authorisations are for specific investigations only, and must be renewed or cancelled once the specific surveillance is complete or about to expire.

   **The authorisations do not lapse with time!**

2. Training Records
   Proper training is given to all Authorised Officers before they are authorised to sign any RIPA Forms. Refresher training will be provided as required. Authorised Officers must ensure that this training is cascaded to ‘Applicants’ within their service area.

3. Application Forms
   Only the approved RIPA forms set out in this Document must be used. The Authorised Officer and/or the Council’s Solicitor will reject any other forms used.

   **Directed Surveillance Forms – Appendix 5**
   Form A Application for Authority to conduct Directed Surveillance
   Form B Review of Directed Surveillance Authority
   Form C Renewal of Directed Surveillance Authority
   Form D Cancellation of Directed Surveillance

   **CHIS Forms – Appendix 6**
   Form E Application for Authority for Conduct and Use of a ‘CHIS’
   Form F Review of Conduct and Use of a ‘CHIS’
   Form G Renewal of Conduct and Use of a ‘CHIS’
   Form H Cancellation of Conduct and Use of a ‘CHIS’
4. **Grounds for Authorisation**

Directed Surveillance *(Forms A-D)* or the Conduct and Use of the CHIS *(Forms E-H)* can only be authorised by the District Council only on one ground:

For the prevention or detection of crime or of preventing disorder. Local authorities can only authorise the use of directed surveillance under RIPA to prevent or detect criminal offences that are punishable whether on summary conviction or indictment by a maximum of at least 6 months’ imprisonment or are related to the underage sale of alcohol or tobacco.

5. **The action to be authorised**

A full description of the proposed surveillance operation must be provided on the form. Plans should be used, where possible, and annexed to the form, particularly where camera surveillance is authorised.

6. **Assessing the Application Form**

Before an Authorised Officer signs a Form, s/he must

a) be mindful of this Corporate Policy & Procedures Document, the Training provided and any other guidance issued, from time to time, by the Senior Responsible Officer and/or Council’s Solicitor on such matters;

b) recognise that s/he should not be responsible for authorising investigations or operations in which they are directly involved, although it is recognised that this may sometimes be unavoidable, especially in the case of small organisations, or where it is necessary to act urgently. Where an Authorising Officer authorises such an investigation or operation the Council’s Solicitor should be advised so that the central record of authorisations can be highlighted to reflect this and the attention of a Commissioner or Inspector can be drawn to it during the next available inspection.

c) Satisfy his/herself that the RIPA authorisation is

- in accordance with the law
- necessary in the circumstances of the particular case on the grounds mentioned in paragraph 4 above, and
- proportionate to what it seeks to achieve

d) Amendments to the Regulation of Investigatory Powers (Directed Surveillance and Covert Human Intelligence Sources) Order 2010 *(the 2010 Order)* mean that a local authority can now only grant an authorisation under RIPA for the use of directed surveillance where the local authority is investigating particular types of criminal offences. These are criminal offences which attract a maximum custodial sentence of six months or more or criminal offences relating to the underage sale of alcohol or tobacco.

The least intrusive method will be considered proportionate by the courts.
e) In assessing whether or not the proposed surveillance is proportionate, consider the seriousness of the matter giving rise to the proposed surveillance and the importance of taking action in respect of it; the implications of not gathering information about the matter; the effects of the proposed surveillance on the subject of the surveillance and on other persons; compare such effects against the seriousness of the matter and the implications of not taking action; indicating what, if any, other action instead of that proposed, might be taken; and confirming whether the action proposed is likely to be the most effective and the least intrusive means of obtaining the required information.

f) Take into account the risk of intrusion into the privacy of persons other than the specified subject of the surveillance (Collateral Intrusion). Measures must be taken wherever practicable to avoid or minimise (so far as is possible) collateral intrusion and the matter may be an aspect of determining proportionality;

g) Ensure authorisation includes name and address of subjects and location of activity with a plan where appropriate;

h) When signing Authorisations:

i) ensure date and time of signature included;

ii) check that a higher level of authority is not required (e.g. confidential information, juvenile sources or use of a vulnerable individual as a source)

i) Set a date for review of the authorisation and review on only that date. Please ensure the authorisation is reviewed regularly, i.e. at least every 4 weeks. Put in place appropriate measures to ensure authorisation is appropriately managed and review date is complied with.

j) Ensure that any RIPA Departmental Register is duly completed, and that a copy of the RIPA Forms (and any review/cancellation of the same) is retained on the departmental file and that the original is forwarded to the Council’s Solicitor within one week of the relevant authorisation, review, renewal, cancellation or rejection.

k) Mark up the departmental file with the URN (unique reference number) on all pages when this is provided by the Council’s Solicitor.

l) In order that the authorisation meets the crime threshold for judicial approval, the Authorising Officer must be satisfied that the requisite crime threshold is satisfied. Examples of cases where the offence being investigated attracts a maximum custodial sentence of 6 months or more could include more serious criminal damage, dangerous waste dumping and serious or serial benefit fraud.

7. Application to a Justice of the Peace

a) A flowchart for an application to a Justice of the Peace seeking an Order to approve the grant of RIPA Authorisation or Notice, is provided at Appendix 3.

b) From 1 November 2012 a local authority who wishes to authorise the use of directed surveillance, acquisition of communications data and the use of a CHIS under RIPA will need to obtain an order approving the grant or renewal of an authorisation or notice from a JP (a District Judge or lay magistrate) before it can take effect. If the JP is satisfied that the statutory tests have been met and that the use of the technique is necessary and proportionate s/he will issue an order approving the grant or renewal for the use of the technique as described in the application.
c) Following approval by the Authorising Officer the first stage of the process is for the investigating officer to contact Her Majesty’s Courts and Tribunals Services (HMCTS) administration team at the Magistrates’ Court to arrange a hearing. The Investigating Officer will provide the JP with a copy of the original RIPA authorisation and the supporting documents setting out the case. This forms the basis of the application to the JP and should contain all information that is relied upon.

d) The original RIPA authorisation should be shown to the JP but will be retained by the local authority so that it is available for inspection by the Commissioners’ Office and in the event of any legal challenge or investigation by the Investigatory Powers Tribunal (IPT). The Court may wish to take a copy. In addition, the Investigating Officer will provide the JP with a partially completed Judicial application/order. “Document Appendix 4”

The order section of this form will be completed by the JP and will be the official record of the JP’s decision. The Investigating Officer will need to obtain judicial approval for all initial RIPA authorisations/applications and renewals and the Council will need to retain a copy of the judicial application/order form after it has been signed by the JP. There is no requirement for the JP to consider either cancellations or internal reviews.

e) On the rare occasions where out of hours access to a JP is required, local arrangements should be made with the relevant HMCTS staff. In these cases, the Investigating Officer will need to provide two partially completed judicial application/order forms so that one can be retained by the JP. The Council should provide the Court with a copy of the signed judicial application/order form the next working day.

f) The hearing is a legal proceeding and therefore local authority officers need to be formally designated under standing orders (under s.223 Local Government Act 1972) to appear, be sworn in and present evidence or provide information as required by the JP.

g) The hearing will be conducted in private and heard by a single JP who will read and consider the RIPA authorisation and the judicial application. S/he may have questions to clarify parts, or require additional assistance.

h) The JP will consider whether s/he is satisfied that at the time the authorisation was granted or renewed, there were reasonable grounds for believing that the authorisation or notice was necessary and proportionate. They will also consider whether there continue to be reasonable grounds. In addition, they must be satisfied that the person who granted the authority or gave the notice was an appropriate designated person within the authority and the authorisation was made in accordance with any applicable legal restrictions, for example that the crime threshold for directed surveillance has been met.

i) Following their consideration of the case, the JP will complete the order section of the Judicial application/order form recording their decision. The JP may decide to 1) approve the grant or renewal of an authorisation or notice 2) refuse to approve the grant or renewal of an authorisation or notice or 3) refuse to approve the grant or renewal and quash the authorisation or notice.

j) There is no complaint route for a judicial decision unless it was made in bad faith. Any complaints should be addressed to the Magistrates’ Advisory Committee. A local authority may only appeal a JP decision point of law by judicial review.

8. Additional Safeguards when Authorising a CHIS
When authorising the conduct or use of a CHIS, the Authorised Officer must also

a) be satisfied that the conduct and/or use of the CHIS is proportionate to what is sought to be achieved;
b) be satisfied that **appropriate arrangements** are in place for the management and oversight of the CHIS and this must address health and safety issues through a risk assessment;

c) consider the likely degree of intrusion of all those potentially affected;

d) consider any adverse impact on community confidence that may result from the use or conduct or the information obtained; and

e) ensure **records** contain particulars and are not available except on a need to know basis

9. **Urgent Authorisations**

The Protection of Freedoms Act 2012 amended the 2000 Act to make local authority authorisations subject to judicial approval. The change means that local authorities need to obtain an order approving the grant or renewal of an authorization from a judicial authority, before it can take effect. The amendment means that local authorities are no longer able to orally authorize the use of RIPA techniques. All authorisations must be made in writing and require JP approval. The authorisation cannot commence until this has been obtained.

10. **Duration**

The Form **must be reviewed in the time stated and cancelled** once it is no longer needed. The ‘authorisation’ to carry out/conduct the surveillance lasts for a maximum of 3 months (from authorisation) for Directed Surveillance (e.g. a Directed Surveillance authorisation granted on 1st April 2005 expires on 30th June 2005) and 12 months (from authorisation) for a CHIS (e.g. a CHIS authorisation granted on 1st April 2005 expires on 31st March 2006). However, whether the surveillance is carried out/conducted or not, in the relevant period, does not mean the ‘authorisation’ is ‘spent’. In other words, the Forms do not expire! The forms have to be reviewed and/or cancelled (once they are no longer required)!

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 (e.g. an urgent authorisation granted at 5.00 pm on 1st June expires at 4.59 pm on 4th June).

Authorisations can be renewed in writing when the maximum period has expired. 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.

The renewal will begin on the day when the authorisation would have expired. In exceptional circumstances, renewals may be granted orally in urgent cases and last for a period of seventy-two hours.

11. **Equipment**

Each department shall keep a record of equipment held and to be used for the purposes of RIPA. A copy of the list of equipment should be forwarded to the Head of Legal Services in order for the central record of all equipment held by the Council to maintained and be kept up to date.

The equipment is to be held by the individual departments should be accessible by other departments within the Council in order to carry out the functions under RIPA. Appropriate training must be given to the individual installing and using the equipment to ensure that the equipment is correctly installed and that data recorded is fit for purpose and meets the objectives of the investigation.

The impact on necessity and/or proportionality will be directed related to the type of equipment used. Any equipment used must be fit for purpose in meeting the objectives of the investigation.
It is therefore important for the authorising officer to be informed of what equipment is being used and its capabilities [i.e. range, how its turned on manually or remotely] on the application form so that due consideration can be given when considering whether or not to grant the authorisation. The authorising officer will also need to give consideration and advise how images will be managed, for example images will not be disclosed without first speaking with the data controller to ensure compliance with the appropriate data protection requirements under the Data Protection Act 1998 and any relevant codes of practice produced by the Council.

When equipment has been installed a check should be undertaken at least every 48 hours if not daily in order to ensure it remains operational.

The Criminal Procedures Investigations Act 1996 Codes of Practice makes provision for the storage and retention of the product of the surveillance. Retention of the investigation data [i.e. images] is to be kept by the relevant department and in accordance with the Codes of Practice and any relevant policy of that Department.

I. Working With / Through Other Agencies

1. If an officer wishes to utilise the CCTV system operated by the CCTV Team a Directed Surveillance Authorisation must be obtained in writing before an approach is made to the Control Room. In exceptional circumstances an urgent authorisation 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. An urgent authorisation will last no more than 72 hours and 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.

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

3. When some other agency (e.g. Police, HM Revenue and Customs etc): -

   a) wishes to use the District Council’s resources (e.g. CCTV surveillance systems), that agency must use its own RIPA procedures and, before any Officer agrees to allow the District Council’s resources to be used for the other agency’s purposes, s/he must obtain a copy of that agency’s RIPA form for the record (a copy of which must be passed to the Council Solicitor for the (Central Register) and/or relevant extracts from the same which are sufficient for the purposes of protecting the District Council and the use of its resources;

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

4. If the Police or other Agency wishes to use District Council resources for general surveillance, as opposed to specific RIPA operations, an appropriate letter requesting the proposed use, extent of remit, duration, who will be undertaking the general surveillance and the purpose of it must be obtained from the Police or other Agency before any District Council resources are made available for the proposed use.

5. If in doubt, please consult with the Senior Responsible Officer at the earliest opportunity.
J. Acquisition And Disclosure Of Communications Data

1.0 Acquisition and Disclosure of Communications Data

1.1 With effect from 5 January 2004, and in accordance with Chapter II of Part 1 of Regulation of Investigatory Powers Act (“the Act”), Local Authorities can authorise the acquisition and disclosure of ‘communications data’ provided that the acquisition of such data is necessary for the purpose of preventing or detecting crime or preventing disorder; and proportionate to what is sought to be achieved by acquiring such data.

Important: The Council is not permitted to Intercept any Communications

1.2 The procedure is similar to that of authorisation for directed surveillance and CHIS but has extra provisions and processes. The purpose and effect of the procedure is the same i.e. to ensure proper consideration is given to permit such investigations and to provide protection against a human rights challenge. The authorising officer is called a ‘designated person’. Judicial approval for the acquisition and disclosure of communications data is required.

2.0 What is ‘Communications Data’?

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

Traffic Data
Where a communication was made from, to whom and when.

Service Data
Use made of service e.g. itemised telephone records.

Subscriber Data
Information held or obtained by operator on person they provide a service to.

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

3.0 Designated Person

3.1 A designated person must be at least the level of Director of equivalent.

4.0 Application Forms

4.1 All applications must be made on a standard form see https://www.gov.uk/government/organisations/home-office/series/ripa-forms--2#this-series
5.0 Authorisations

5.1 Authorisations can only authorise conduct to which Chapter II of Part I of the Act applies. In order to comply with the code, a designated person can only authorise the obtaining and disclosure of communications data if:

i) It is necessary for any of the purposes set out in Section 22(2) of the Act. (NB the Council can only authorise for the purpose set out in Section 22(2)(b) which is the purpose of preventing or detecting crime or preventing disorder); and

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

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

5.2 Once a designated person has decided to grant an authorisation or a notice and judicial approval has been granted there are two methods:-

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

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

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

5.3 The Service provider must comply with the notice if it is reasonably practicable to do so (s.22 (6)-(8) and can be enforced to do so by civil proceedings. The postal or telecommunications service can charge for providing this information. There are standard forms see https://www.gov.uk/government/organisations/home-office/series/ripa-forms--2#this-series for authorisations and notice.

6.0 Oral Authority

6.1 The Council is not permitted to apply or approve orally.

7.0 Single Point of Contact (SPOC)

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

- Where appropriate, assess whether access to communication data is reasonably practical for the postal or telecommunications operator;
- Advise applicants and designated person on whether communications data falls under Section 21(4)(a), (b) or (c) of the Act;
- Provide safeguards for authentication;
- Assess any cost and resource implications to both the public authority and the postal or telecommunications operator.

7.3 A SPOC must be accredited which involves undertaking appropriate training. The Council currently has no SPOC and does not currently envisage circumstances where it would be necessary for the Council to authorise the acquisition and disclosure of communications data. However, this aspect of the Policy will be regularly reviewed.

8.0 Duration

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

9.0 Renewal and Cancellation

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

9.2 The code requires that all authorisations and notices should be cancelled by the designated person who issued it as soon as it is no longer necessary, or the conduct is no longer proportionate to which is sought to be achieved. The relevant postal or telecommunications operator should be informed of the cancellation of a notice.

10.0 Retention of Records

10.1 Applications, authorisations and notices must be retained until the Council has been audited by the Commissioner (see paragraph 9). Applications must also be retained to allow the Tribunal (see paragraph 9) to carry out its functions.

10.2 A record must be kept of:

- The date of which the authorisation or notice is started or cancelled;
- Any errors that have occurred in the granting of authorisations or giving of notices.

A report and explanation of any errors must also be sent to the Commissioner as soon as is practicable. Communications data, and all copies, extracts and summaries of it, must be handled and stored securely and the requirements of the Data Protection Act 1998 must be observed. The Director of Safety will maintain a centrally retrievable register.

11.0 Oversight and Complaints

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

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

K. Records Management

1. The District Council must keep a detailed record of all authorisations; renewals, cancellations and rejections in Departments and a Central Register of all Authorisation Forms will be maintained and monitored by the Council’s Solicitor

2. Records maintained in the Department

   The following documents must be retained by the relevant Authorised Officer (or his/her designated Departmental Co-ordinator)

   • a copy of the Forms 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 supporting documentation submitted when the renewal was requested;
   • the date and time when any instruction was given by the Authorised Officer;
   • the Unique Reference Number for the authorisation (URN) supplied by the Council’s Solicitor

3. Each form will have a URN. The Council’s Solicitor will issue the relevant URN to Applicants.

4. Product from Directed Surveillance

   Material obtained as a result of surveillance activities e.g. photographs; video film; surveillance log; officers notes, should be recorded on a record. A copy of this record should be given to the Authorised Officer to be filed with the Authorisation Form. The Applicant or Investigating Officer should retain the original on the case or investigation file. All Officers should ensure that the integrity, security and confidentiality of this material is maintained. Such material should be retained for a period of no more than five years. If the material is no longer required it should where possible be destroyed sooner. When it is destroyed, this fact should be recorded on the original record and be signed by the relevant Officer. A copy of the amended record should then be given to the Authorised Officer.

5. Records of Use and Product from a CHIS

   Similarly for Directed Surveillance records, records of the use and of the materials provided by a CHIS should be maintained by the Applicant and Authorised Officer, for a period of no longer than five years in the manner set out above.

6. Central Register maintained by Senior Responsible Officer

   Authorised Officers must forward originals of each Form to the Senior Responsible Officer c/o the
Council Solicitor for the Central Register, within 1 week of the authorisation, review, renewal, cancellation or rejection. The Senior Responsible Officer will monitor the same and give appropriate guidance, from time to time, or amend this Document, as necessary. The Senior Responsible Officer and those authorised by him will have access to the Central Register which will be held in the locked strong room within the Council Solicitor’s Department.

7. The District Council will retain records for a period of at least three years from the ending of the authorisation. The Office of the Surveillance Commissioners (OSC) can audit/review the District Council’s policies and procedures, and individual authorisations.

L. Complaints

1. Copies of the Codes of Practice on Covert Surveillance and Covert Human Intelligence Sources will be made available to the public by request to the Council Solicitor at Queen’s Buildings, Potter Street, Worksop, Nottinghamshire S80 2AH or by telephoning 01909 533 456. Access can also be provided, on request, to the Regulation of Investigatory Powers Act 2000 and related regulations.

2. Complaints about the Council’s actions under RIPA should be submitted in writing to the Council Solicitor at the above address.

3. Information on the Investigatory Powers Tribunal will be provided as part of the response to any RIPA complaint, including the provision of copies of the Tribunal’s complaint form and information leaflet, or by contacting the Council Solicitor as indicated above.

4. This Corporate Policy and Procedures Document is available on the Council’s website at www.bassetlaw.gov.uk and is contained in the Council’s Publication Scheme.

M. Summary

1. Where there is an interference with the right to respect for private life and family guaranteed under Article 8 of the European Convention on Human Rights, and where there is no other source of lawful authority for the interference, or if it is held not to be necessary or proportionate to the circumstances, the consequences of not obtaining or following the correct authorisation procedure may be that the action (and the evidence obtained), is held to be inadmissible by the Courts pursuant to Section 6 of the Human Rights Act 1998.

2. Obtaining an authorisation under RIPA and following 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.

3. Authorised Officers will be suitably trained and they 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 the District Council’s responsibilities.

4. Any boxes not needed on the Form(s) must be clearly marked as being ‘NOT APPLICABLE’, ‘N/A’ or a line put through the same. Great care must also be taken to ensure accurate information is used and is inserted in the correct boxes. Reasons for any refusal of an application must also be kept on the form and the form retained for future audits.

5. Particular care must be taken when considering and confirming whether the proposed surveillance is proportionate to what it seeks to achieve. The explanation must be full and complete.
6. Authorised Officers, in giving approval, must state on the form, in detail, why they consider the proposed action to be necessary and proportionate.

7. Care must also be taken to ensure that a full description of the surveillance operation is given on the authorisation form. Appropriate plans, should be used, particularly where camera surveillance is proposed.

8. The use of “cut and paste” entries on Authorisations is not advised without careful attention to detail, accuracy and pertinence.

9. Investigating and Authorised Officers should note that the expiry date (date for cancellation) for an authorisation for Directed Surveillance lasting three months commencing, e.g. on 1 March is 31 May and not 1 June.

10. Authorised activities, and therefore authorisations, should be regularly reviewed, i.e. at least every 4 weeks.

11. For further advice and assistance on RIPA, please contact the Senior Responsible Officer. Details are provided on the front of this document.

APPENDIX 1

List of Authorised Officer Posts

Chief Executive
Director of Corporate Resources
Director of Regeneration and Neighbourhoods
Head of Corporate Services
APPENDIX 2

RIPA Flow Chart

**Requesting Officer must**
- Read Policy & Procedure document and other guidance
- Determine the nature of surveillance
- Assess whether authorisation will be in accordance with the law
- Assess whether authorisation is necessary under RIPA and if it could be done overtly
- Consider if surveillance is proportionate
- If approved – review regularly

If a less intrusive option is available and practicable

If authorisation is necessary and proportionate, prepare and submit an approved form(s) to the Magistrates Court (personal appearance by requesting officer)

Not authorised by Magistrates Court – No further action

Submit authorised forms to AO for approval by BDC

**Authorised Officer (AO) must**
- Consider in detail whether all options have been duly considered
- Consider whether surveillance is necessary and proportionate
- Authorise only if an overt or less intrusive option is not practicable
- Set an appropriate review date (can be up to 3 months after authorisation date) and conduct the review

The applicant must
- Review regularly
- Complete Review Form
- Submit form to AO

The Applicant must if operation is no longer necessary or proportionate
- Complete Cancellation Form
- Submit form to AO

Authorised Officer must if surveillance still necessary and proportionate
- Review authorisation
- Set an appropriate further review date

Authorised Officer must
- Cancel authorisation when it is no longer necessary or proportionate

Essential:
Send all Authorised (and any rejected) forms, Reviews, Renewals and Cancellations to the Senior Responsible Officer within one week of the relevant event
APPENDIX 3

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

Local authority investigator wants to use a RIPA technique (directed surveillance, CHIS (covert human intelligence source) or communications data).

Does investigator intend to use directed surveillance?

- YES
- NO

Is the local authority investigating an offence and does that offence attract a maximum custodial sentence of 6 months or more?

- NO
- YES

Is the offence being investigated either:
  - Section 146/147/147A of the Licensing Act 2003, or
  - Section 7 of the Children and Young Persons Act 1993

- NO
- YES

Within Office Hours

Local authority investigator to contact Her Majesty’s Courts & Tribunals Service (HMCTS) administration at the magistrates’ court to arrange a hearing.

Attend court with:

- Counter-signed RIPA authorisation/or notice (for CD authorisations/notices the signatures may be electronic signatures)
- The accompanying judicial application/order form
- Any other relevant reference or supporting material

Outside usual office hours:

A JP may consider an authorisation out of hours in exceptional circumstances. If the authorisation is urgent and cannot be handled the next working day then you should:

- Phone the court’s out of hours HMCTS legal staff contact. You will be asked about the basic facts and urgency of the authorisation. If the police are involved in the investigation you will need to address why they cannot make a RIPA authorisation
- If urgency is agreed, then arrangements will be made for a suitable JP to consider the application. You will be told where to attend and give evidence.
- Attend hearing as directed with two copies of both the countersigned RIPA authorisation form or notice and the accompanying judicial application/order form

Investigator may not use directed surveillance. The case should be investigated by other means. Continue to assess if threshold is met if further offences come to light as the case progresses.

Outcome

- Refuse to approve the grant or renewal and quash the authorisation or notice as the case progresses
- Approve the grant or renewal of an authorisation or notice
- Approve the grant or renewal of an authorisation or notice
- Technique may be used in this case. Investigator to resubmit to the JP any renewal or authorisation for the use of a different technique in this case

Refuse to approve the grant or renewal of an authorisation or notice

- The grant or renewal of the RIPA authorisation or notice will not take effect and the local authority may not use the covert technique. Local authority may wish to address, for example, a technical error and reapply

Obtain signed order and retain original RIPA authorisation/notice.

For CD authorisations or notices, local authority investigator to provide additional copy of judicial order to the SPoC.

If out of hours, a copy of the signed order to be provided to the court the next day
Application for judicial approval for authorisation to obtain or disclose communications data, to use a covert human intelligence source or to conduct directed surveillance. Regulation of Investigatory Powers Act 2000 sections 23A, 23B, 32A, 32B.

Local authority: ........................................................................................................................................................................
Local authority department: ...................................................................................................................................................................
Offence under investigation: ....................................................................................................................................................................
Address of premises or identity of subject: ..................................................................................................................................................

Covert technique requested: (tick one and specify details)

Communications Data ☐
Covert Human Intelligence Source ☐
Directed Surveillance ☐

Summary of details

...................................................................................................................................................................................................
...................................................................................................................................................................................................
...................................................................................................................................................................................................
...................................................................................................................................................................................................
...................................................................................................................................................................................................
...................................................................................................................................................................................................

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

Investigating Officer: ........................................................................................................................................................................
Authorising Officer/Designated Person: ...................................................................................................................................................
Officer(s) appearing before JP: .........................................................................................................................................................
Address of applicant department: ...........................................................................................................................................................

Contact telephone number: ....................................................................................................................................................................
Contact email address (optional): ............................................................................................................................................................
Local authority reference: ........................................................................................................................................................................
Number of pages: .................................................................................................................................................................................
Order made on an application for judicial approval for authorisation to obtain or disclose communications data, to use a covert human intelligence source or to conduct directed surveillance. Regulation of Investigatory Powers Act 2000 sections 23A, 23B, 32A, 32B.

Magistrates’ court: ..........................................................................................................................................................................................................................................

Having considered the application, I (tick one):

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

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

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

Notes
..........................................................................................................................................................................................................................................
..........................................................................................................................................................................................................................................
..........................................................................................................................................................................................................................................
..........................................................................................................................................................................................................................................
..........................................................................................................................................................................................................................................

Reasons
..........................................................................................................................................................................................................................................
..........................................................................................................................................................................................................................................
..........................................................................................................................................................................................................................................
..........................................................................................................................................................................................................................................
..........................................................................................................................................................................................................................................

Signed:
Date:
Time:
Full name:
Address of magistrates’ court:
APPENDIX 5

DIRECTED SURVEILLANCE FORMS

A - Application for authority to conduct Directed Surveillance
B - Review of a Directed Surveillance authorisation
C - Application to renew authorisation for Directed Surveillance
D - Cancellation of a Directed Surveillance authorisation

Authorisation Directed Surveillance

<table>
<thead>
<tr>
<th>Public Authority</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>(including full address)</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Name of Applicant</th>
<th>Unit/Branch /Division</th>
</tr>
</thead>
</table>

| Full Address |  |
|--------------|  |

| Contact Details |  |
|----------------|  |

| Investigation/Operation Name (if applicable) |  |
|---------------------------------------------|  |

| Investigating Officer (if a person other than the applicant) |  |
Form A

Unique Reference Number

1. Give rank or position of authorising officer in accordance with the Regulation of Investigatory Powers (Directed Surveillance and Covert Human Intelligence Sources) Order 2010 No. 521.¹

2. Describe the purpose of the specific operation or investigation.

3. Describe in detail the surveillance operation to be authorised and expected duration, including any premises, vehicles or equipment (e.g. camera, binoculars, recorder) that may be used.

4. The identities, where known, of those to be subject of the directed surveillance.

   • Name:
   • Address:
   • DOB:
   • Other information as appropriate:

¹ For local authorities: The exact position of the authorising officer should be given. For example, Head of Trading Standards.
5. Explain the information that it is desired to obtain as a result of the directed surveillance.

6. Identify on which grounds the directed surveillance is necessary under Section 28(3) of RIPA. Delete those that are inapplicable. Ensure that you know which of these grounds you are entitled to rely on (*SI 2010 No.521*).

- In the interests of national security;
- **For the purpose of preventing or detecting crime**¹ or of preventing disorder;
- In the interests of the economic well-being of the United Kingdom;
- In the interests of public safety;
- for the purpose of protecting public health;
- for the purpose of assessing or collecting any tax, duty, levy or other imposition, contribution or charge payable to a government department;

¹ Local Authorities can only authorize the use of directed surveillance under RIPA to prevent or detect criminal offences that are either (a) punishable by a maximum term of imprisonment of at least six months, or (b) are related to the underage sale of alcohol and tobacco.

7. Explain why this directed surveillance is necessary on the grounds you have identified [Code paragraph 3.3].
8. Supply details of any potential collateral intrusion and why the intrusion is unavoidable. [Bear in mind Code paragraphs 3.8 to 3.11.]
Describe precautions you will take to minimise collateral intrusion.

9. Explain why this directed surveillance is proportionate to what it seeks to achieve. How intrusive might it be on the subject of surveillance or on others? And why is this intrusion outweighed by the need for surveillance in operational terms or can the evidence be obtained by any other means [Code paragraphs 3.4 to 3.7]?

10. Confidential information [Code paragraphs 4.1 to 4.31].
INDICATE THE LIKELIHOOD OF ACQUIRING ANY CONFIDENTIAL INFORMATION:
11. Applicant’s Details

<table>
<thead>
<tr>
<th>Name (print)</th>
<th>Tel No:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Grade/Rank</td>
<td>Date</td>
</tr>
<tr>
<td>Signature</td>
<td></td>
</tr>
</tbody>
</table>

12. Authorising Officer’s Statement. [Spell out the “5 Ws” – Who; What; Where; When; Why and HOW– in this and the following box. ]

I hereby authorise directed surveillance defined as follows: [Why is the surveillance necessary, whom is the surveillance directed against, Where and When will it take place, What surveillance activity/equipment is sanctioned, How is it to be achieved?]
13. Explain **why** you believe the directed surveillance is necessary [Code paragraph 3.3]. Explain **why** you believe the directed surveillance to be proportionate to what is sought to be achieved by carrying it out [Code paragraphs 3.4 to 3.7].

<table>
<thead>
<tr>
<th>Date of first review</th>
</tr>
</thead>
</table>

14. (Confidential Information Authorisation.) Supply detail demonstrating compliance with Code paragraphs 4.1 to 4.31.

<table>
<thead>
<tr>
<th>Date of first review</th>
</tr>
</thead>
</table>

Programme for subsequent reviews of this authorisation: [Code paragraph 3.23]. Only complete this box if review dates after first review are known. If not or inappropriate to set additional review dates then leave blank.

<table>
<thead>
<tr>
<th>Name (Print)</th>
<th>Grade / Rank</th>
</tr>
</thead>
<tbody>
<tr>
<td>Signature</td>
<td>Date and time</td>
</tr>
</tbody>
</table>

Expiry date and time [ e.g.: authorisation granted on 1 April 2005 - expires on 30 June 2005, 23.59 ]
Form A

15. Urgent Authorisation [Code paragraph 5.9]: Authorising officer: explain why you considered the case so urgent that an oral instead of a written authorisation was given.

16. If you are only entitled to act in urgent cases: explain why it was not reasonably practicable for the application to be considered by a fully qualified authorising officer.

<table>
<thead>
<tr>
<th>Name (Print)</th>
<th>Grade / Rank</th>
</tr>
</thead>
<tbody>
<tr>
<td>Signature</td>
<td>Date and time</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Urgent authorisation</th>
<th>Expiry date:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Expiry time:</td>
</tr>
</tbody>
</table>

Remember the 72 hour rule for urgent authorities – check Code of Practice.

e.g. authorisation granted at 5pm on June 1st expires 4.59pm on 4th June
Form E

CHIS Unique Reference Number (URN) (to be supplied by the central monitoring officer).

**Part II of the Regulation of Investigatory Powers Act 2000**

**Review of a Directed Surveillance authorisation**

<table>
<thead>
<tr>
<th>Public Authority</th>
<th>Unit/Branch /Division</th>
</tr>
</thead>
<tbody>
<tr>
<td>(including full address)</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Name of Applicant</th>
<th>Unit/Branch /Division</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

| Full Address | |
|--------------||
| | |

| Contact Details | |
|-----------------||
| | |

<table>
<thead>
<tr>
<th>Operation Name</th>
<th>Operation Number*</th>
</tr>
</thead>
<tbody>
<tr>
<td>Operation Number*</td>
<td>*Filing Ref</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Date of authorisation or last renewal</th>
<th>Expiry date of authorisation or last renewal</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Review Number</td>
</tr>
</tbody>
</table>

**Details of review:**

1. Review number and dates of any previous reviews.

<table>
<thead>
<tr>
<th>Review Number</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>
### Form E

**CHIS Unique Reference Number (URN)**
(to be supplied by the central monitoring officer).

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>2.</strong> Summary of the investigation/operation to date, including what private information has been obtained and the value of the information so far obtained.</td>
<td></td>
</tr>
<tr>
<td><strong>3.</strong> Detail the reasons why it is necessary to continue with the directed surveillance.</td>
<td></td>
</tr>
<tr>
<td><strong>4.</strong> Explain how the proposed activity is still proportionate to what it seeks to achieve.</td>
<td></td>
</tr>
<tr>
<td><strong>5.</strong> Detail any incidents of collateral intrusion and the likelihood of any further incidents of collateral intrusions occurring.</td>
<td></td>
</tr>
<tr>
<td><strong>6.</strong> Give details of any confidential information acquired or accessed and the likelihood of acquiring confidential information.</td>
<td></td>
</tr>
</tbody>
</table>
Form E
CHIS Unique Reference Number (URN) (to be supplied by the central monitoring officer).

7. Applicant’s Details

<table>
<thead>
<tr>
<th>Name (Print)</th>
<th>Tel No</th>
</tr>
</thead>
<tbody>
<tr>
<td>Grade/Rank</td>
<td>Date</td>
</tr>
<tr>
<td>Signature</td>
<td></td>
</tr>
</tbody>
</table>

8. Review Officer’s Comments, including whether or not the directed surveillance should continue.

9. Authorising Officer’s Statement.

I, [insert name], hereby agree that the directed surveillance investigation/operation as detailed above [should/should not] continue [until its next review/renewal][it should be cancelled immediately].

<table>
<thead>
<tr>
<th>Name (Print)</th>
<th>Grade / Rank</th>
</tr>
</thead>
<tbody>
<tr>
<td>Signature</td>
<td>Date</td>
</tr>
</tbody>
</table>

10. Date of next review.
Form E

CHIS Unique Reference Number (URN)
(to be supplied by the central monitoring officer).


Renewal of a Directed Surveillance Authorisation

<table>
<thead>
<tr>
<th>Public Authority</th>
<th>Unit/Branch /Division</th>
</tr>
</thead>
<tbody>
<tr>
<td>(including full address)</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Name of Applicant</th>
<th>Unit/Branch /Division</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Full Address</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Contact Details</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Investigation/Operation Name (if applicable)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Renewal Number</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
</tr>
</tbody>
</table>

Details of review:

1. Review number and dates of any previous reviews.

<table>
<thead>
<tr>
<th>Review Number</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

www.bassetlaw.gov.uk
Form E

CHIS Unique Reference Number (URN)  
(to be supplied by the central monitoring officer).

2. Detail any significant changes to the information as listed in the original authorisation as it applies at the time of the renewal.

3. Detail the reasons why it is necessary to continue with the directed surveillance.

4. Detail why the directed surveillance is still proportionate to what it seeks to achieve.

5. Indicate the content and value to the investigation or operation of the information so far obtained by the directed surveillance.

6. Give details of the results of the regular reviews of the investigation or operation.

7. Applicant’s Details

<table>
<thead>
<tr>
<th>Name (Print)</th>
<th>Tel No</th>
</tr>
</thead>
<tbody>
<tr>
<td>Grade/Rank</td>
<td>Date</td>
</tr>
<tr>
<td>Signature</td>
<td></td>
</tr>
</tbody>
</table>
8. Authorising Officer’s Comments. This box must be completed.


9. Authorising Officer’s Statement.

I, [insert name], hereby agree that the directed surveillance investigation/operation as detailed above [should/should not] continue [until its next review/renewal][it should be cancelled immediately].

Name (Print) ................................................................. Grade / Rank ..................................................

Signature ................................................................. Date .............................................................

Renewal From:       Time:       Date:

Date of first review.

Date of subsequent reviews of this authorisation.

Cancellation of a Directed Surveillance authorisation

<table>
<thead>
<tr>
<th>Public Authority</th>
<th>Unit/Branch /Division</th>
</tr>
</thead>
<tbody>
<tr>
<td>(including full address)</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Name of Applicant</th>
<th>Full Address</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Contact Details</th>
<th>Investigation/Operation Name (if applicable)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Details of cancellation:

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

CHIS Unique Reference Number (URN) (to be supplied by the central monitoring officer).

2. Explain the value of surveillance in the operation:

<table>
<thead>
<tr>
<th>Date:</th>
<th>Date:</th>
<th>Date:</th>
<th>Date:</th>
</tr>
</thead>
</table>

3. Authorising officer’s statement.

I, [insert name], hereby agree that the directed surveillance investigation/operation as detailed above [should/should not] continue [until its next review/renewal][it should be cancelled immediately].

Name (Print) ....................................................................... Grade / Rank ..........................................

Signature ............................................................................   Date ........................................................

4. Time and Date of when the authorising officer instructed the surveillance to cease.

   Date:                  Date:                  Date:                  Date:                  Date:                  

5. Authorisation cancelled.

6. Authorisation cancelled.

7. Authorisation cancelled.

8. Authorisation cancelled.
Form E
CHIS Unique Reference Number (URN)
(to be supplied by the central monitoring officer).

APPENDIX 6

CHIS FORMS

E - Application for authority to conduct CHIS Surveillance

F - Review of a CHIS authorisation

G - Application for renewal of a CHIS authorisation

H - Cancellation of authority for the Use or Conduct of a CHIS
# Part II of the Regulation of Investigatory Powers Act 2000

Application for authorisation of the conduct or use of a Covert Human Intelligence Source (CHIS)

<table>
<thead>
<tr>
<th>Public Authority</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>(including full address)</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Name of Applicant</th>
<th>Service/Department/Branch</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>How will the source be referred to (i.e. what will be his/her pseudonym or reference number)?</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>What is the name, rank or position of the person within the relevant investigating authority who will have day to day responsibility for dealing with the source, including the source’s security and welfare (often referred to as the Handler)?</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>What is the name, rank or position of another person within the relevant investigating authority who will have general oversight of the use made of the source (often referred to as the Controller)?</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Who will be responsible for retaining (in secure, strictly controlled conditions, with need-to-know access) the source’s true identity, a record of the use made of the source and the particulars required under RIP (Source Records) Regulations 2000 (SI 2000/2725)?</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Investigation/Operation Name (if applicable)</th>
<th></th>
</tr>
</thead>
</table>
# DETAILS OF APPLICATION

1. Give rank or position of authorising officer in accordance with the Regulation of Investigatory Powers (Directed Surveillance and Covert Human Intelligence Sources) Order 2010 No. 521.\(^1\) Where appropriate throughout amend references to the Order relevant to your authority.

2. Describe the purpose of the specific operation or investigation.

3. Describe in detail the purpose for which the source will be tasked or used.

4. Describe in detail the proposed covert conduct of the source or how the source is to be used.

5. Identify on which grounds the conduct or the use of the source is necessary under Section 29(3) of RIPA. Delete those that are inapplicable. Ensure that you know which of these grounds you are entitled to rely on (eg. SI 2010 No.521).

   - In the interests of national security;
   - For the purpose of preventing or detecting crime or of preventing disorder;
   - In the interests of the economic well-being of the United Kingdom;
   - In the interests of public safety;
   - for the purpose of protecting public health;
   - for the purpose of assessing or collecting any tax, duty, levy or other imposition, contribution or charge payable to a government department.

---

\(^1\) For local authorities: The formal position of the authorising officer should be given. For example, Head of Trading Standards.
6. Explain why this conduct or use of the source is necessary on the grounds you have identified [Code paragraph 3.2].

| 7. Supply details of any potential collateral intrusion and why the intrusion is unavoidable. [Bear in mind Code paragraphs 3.8 to 3.11.] Describe precautions you will take to minimise collateral intrusion and how any will be managed. |

| 8. Are there any particular sensitivities in the local community where the source is to be used? Are similar activities being undertaken by other public authorities that could impact on the deployment of the source (see Code paragraphs 3.17 to 3.18)? |

| 9. Provide an assessment of the risk to the source in carrying out the proposed conduct (see Code paragraph 6.14). |
Form E

CHIS Unique Reference Number (URN)
(to be supplied by the central monitoring officer).

9. Provide an assessment of the risk to the source in carrying out the proposed conduct (see Code paragraph 6.14).

10. Explain why this conduct or use of the source is proportionate to what it seeks to achieve. How intrusive might it be on the subject(s) of surveillance or on others? How is this intrusion outweighed by the need for a source in operational terms, and could the evidence be obtained by any other means [Code paragraphs 3.3 to 3.5]?

11. Confidential information [Code paragraphs 4.1 to 4.21]
Indicate the likelihood of acquiring any confidential information.

References for any other linked authorisations:

12. Applicant’s Details.

<table>
<thead>
<tr>
<th>Name (print)</th>
<th>Grade/Rank/Position</th>
</tr>
</thead>
<tbody>
<tr>
<td>Signature</td>
<td>Tel No:</td>
</tr>
</tbody>
</table>

Date
Contact us

01909 533 533
www.bassetlaw.gov.uk
customer.services@bassetlaw.gov.uk
Text us on 07797 800 573
Find us on Facebook - BassetlawDC
Twitter @BassetlawDC
Visit us at:
Retford One Stop Shop
17B The Square, Retford DN22 6DB
Worksop One Stop Shop
Queens Buildings, Potter Street, Worksop S80 2AH
All offices are open: Monday to Friday 9:00am to 5:00pm

If you need any help communicating with us or understanding any of our documents, please contact us on 01909 533 533.

We can arrange for a copy of this document in large print, audiotape, Braille or for a Language Line interpreter to help you.