REGULATION OF INVESTIGATORY POWERS ACT 2000

Use of Covert Directed Surveillance

Use of Covert Human Intelligence Sources

Accessing Communications Data

POLICY OF WREXHAM COUNTY BOROUGH COUNCIL AND GUIDANCE TO EMPLOYEES

Policy Date: June 2015
Review Date: 9 January 2018
## INDEX OF CONTENTS

<table>
<thead>
<tr>
<th>Part 1 – Introduction</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.1 Covert Surveillance and Covert Human Intelligence Sources</td>
<td>3</td>
</tr>
<tr>
<td>1.2 Access to Communications Data</td>
<td></td>
</tr>
<tr>
<td>1.3 Purpose of Policy</td>
<td>4</td>
</tr>
<tr>
<td>1.4 Implementation</td>
<td></td>
</tr>
<tr>
<td>1.5 Basic Requirements</td>
<td></td>
</tr>
<tr>
<td>1.6 Training</td>
<td>5</td>
</tr>
<tr>
<td>1.7 Data Protection and Freedom of Information</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Part 2 – Surveillance</th>
<th>6</th>
</tr>
</thead>
<tbody>
<tr>
<td>2.1 Types of Surveillance</td>
<td></td>
</tr>
<tr>
<td>2.2 Authorisation</td>
<td>7</td>
</tr>
<tr>
<td>2.3 Equipment</td>
<td></td>
</tr>
<tr>
<td>2.4 Risk Assessments and Health &amp; Safety</td>
<td>8</td>
</tr>
<tr>
<td>2.5 Authorising Officers</td>
<td></td>
</tr>
<tr>
<td>2.6 Evidence</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Part 3 – Covert Human Intelligence Source</th>
<th>10</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.1 Definition</td>
<td></td>
</tr>
<tr>
<td>3.2 Authorisation</td>
<td></td>
</tr>
<tr>
<td>3.3 Management of the source</td>
<td>11</td>
</tr>
<tr>
<td>3.4 Record keeping</td>
<td>12</td>
</tr>
<tr>
<td>3.5 Safety &amp; Security</td>
<td>13</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Part 4 – Requesting Authorisation to use covert surveillance/CHIS</th>
<th>14</th>
</tr>
</thead>
<tbody>
<tr>
<td>4.1 Procedure</td>
<td></td>
</tr>
<tr>
<td>4.2 Confidential Information and Role of Authorising Officers</td>
<td></td>
</tr>
<tr>
<td>4.3 Reviews, renewals and cancellations</td>
<td>15</td>
</tr>
</tbody>
</table>

| Part 5 – Central Record | 16 |

| Part 6 – Requests for Council Officers to undertake Surveillance | 17 |

<table>
<thead>
<tr>
<th>Part 7 – Access to Communications Data</th>
<th>18</th>
</tr>
</thead>
<tbody>
<tr>
<td>7.1 Introduction and types of communications data</td>
<td></td>
</tr>
<tr>
<td>7.2 Designated Persons</td>
<td></td>
</tr>
<tr>
<td>7.3 Single Point of Contact</td>
<td></td>
</tr>
<tr>
<td>7.4 Procedure</td>
<td>19</td>
</tr>
<tr>
<td>7.5 Errors</td>
<td></td>
</tr>
</tbody>
</table>

| Part 8 – Surveillance by use of Social Media | 20 |

| Part 9 – Complaints | 21 |

<table>
<thead>
<tr>
<th>Appendices</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Appendix 1 – List of Authorising Officers Posts</td>
<td>22</td>
</tr>
<tr>
<td>Appendix 2 – Single Point of Contact and List of Designated Person Posts</td>
<td></td>
</tr>
<tr>
<td>Appendix 3 – Guidance to Staff – Completion of RIPA1 Form</td>
<td>23</td>
</tr>
<tr>
<td>Appendix 4 – Flowchart – Do you need authorisation?</td>
<td>29</td>
</tr>
</tbody>
</table>
PART 1 - Introduction

1.1 Covert Surveillance and Human Intelligence Sources

Some of the Council’s activities will necessarily require covert surveillance as part of their enforcement functions. Examples include Environment and Public Protection noise complaint investigations, Trading Standards investigations, planning or licensing enforcement. The Regulation of Investigatory Powers Act 2000 provides the statutory framework for the operation of Covert Surveillance or use of Covert Human Intelligence Sources (also known as “CHIS”).

The Council is fully committed to complying with the Human Rights Act 1998 (HRA) and the Regulation of Investigatory Powers Act 2000 (RIPA – the Act). To ensure compliance, all use of covert surveillance and of covert human intelligence sources, by officers of the Council (or agents acting on its behalf), falling within the scope of the Act, must be carried out with authorisation from a designated ‘Authorising Officer’ in the form prescribed in the procedure. In addition, as a result of changes introduced by the Protection of Freedoms Act 2012, approval must also be sought from the Magistrates Court to permit the regulated activity to take place. The advice and approval of the Council’s Legal Services section should be obtained regarding the content of any application for authorisation and application to Court for Judicial approval.

In complying with RIPA, officers must have full regard to the relevant Codes of Practice issued by the Home Office. The Codes are available on the RIPA page of the Council’s intranet site and there is a link to the relevant Home Office web page.

1.2 Access to Communication Data

In addition to covert surveillance or use of CHIS, Local Authority’s investigating criminal offences have powers (by virtue of The Regulation of Investigatory Powers (Communications Data) Order 2010 (“the Order”) to gain access to communications data – that is, information held by telecommunication or postal service providers about the use of their services by persons who are the subject of criminal investigations (such information would not include the content of a communication however).

In using such powers, officers must have full regard to the Code of Practice on Accessing Communications Data, issued by the Home Office. As with covert surveillance, access to communications data must be authorised by a designated ‘Authorising Officer’, obtained via the Council’s ‘Single Point of Contact’ (SPOC) and approved by Order of the Magistrates’ Court. More information about this is contained in part 7 of this policy. Again the advice and approval of the Council’s Legal Services section should be obtained regarding the content of any application for authorisation and application to Court for Judicial approval.

There is also provision in RIPA for interception of communications but those powers are not generally available to local authorities.
1.3 Purpose of the Policy

It is essential that all activities of this nature, whether they will lead to prosecution or not, are carried out in accordance with the Act and associated legislation, the Home Office Codes of Practice and this policy. Investigations which fall within the scope of the Act, which are not authorised, may be a breach of s 6 of the Human Rights Act 1998 and could leave the Council open to legal challenge by individuals who consider that there has been an intrusion into their privacy, or in a prosecution, evidence might be excluded by the court as being inadmissible.

The purpose of this document is to set out the Council’s policy and procedure on RIPA, to reinforce the requirements of the Act, the Order and Codes of Practice, to provide guidance to employees, to protect the rights of individuals and to minimise the risk of legal challenge as a result of officer actions.

Each investigation where the use of covert surveillance, CHIS or access to communications data is requested must be subject to a separate authorisation request.

Any failure to comply with the procedures in place for the implementation of this policy will be a disciplinary offence.

1.4 Implementation

The Council’s Policy has been developed in consultation with representatives from across those departments of the Council which make use (or are likely to make use) of the powers conferred by RIPA.

The Council’s Policy is operational forthwith, replacing any previous policies and procedures. It will apply to all Council staff and contractors employed by the Council. All relevant Council contracts will include a term that this Policy and the Council’s associated procedures are to be observed by any contractor operating on behalf of the Council.

A copy of this Policy Document together with the Home Office Codes of Practice and Investigatory Powers Tribunal leaflets will be made available for Public Inspection at Council Offices.

1.5 Basic Requirements

Under the Act, the Order and Home Office Codes of Practice, directed covert surveillance, use of CHIS and access to communications data should only be authorised if the authorising officer is satisfied that:

- The action is NECESSARY for the prevention or detection of crime or the prevention of disorder.

- The surveillance/access to communications data is PROPORTIONATE – a measure or action is proportionate if it:
  - Impairs as little as possible the rights and freedoms (of the individual concerned and of innocent third parties).
- Is carefully designed to meet the objectives in question, is not arbitrary, unfair or based on irrational consideration.

AND, in the case of directed surveillance only, the crime threshold must be met (i.e. the offence under investigation must attract a term of imprisonment of at least 6 months or relate to the underage sale of alcohol or tobacco).

More guidance on the requirements of the crime threshold and necessity and proportionality for directed surveillance is contained in Appendix 3 to this policy (Guidance on Completion of RIPA1 Application Form).

1.6 Training

All Investigators and Authorising Officers MUST BE trained on the provisions of RIPA to ensure that the requirements of the law are complied with.

1.7 Data Protection and Freedom of Information

Officers and others using this policy and the powers under RIPA must ensure that the use and storage of any personal information obtained by these methods must be undertaken in accordance with the Data Protection Act 1998 and from the 25 May 2018, the General Data Protection Regulation 2016. Officers must also take account of the impact of the Freedom of Information Act 2000 and the Environmental Information Regulations 2004 in respect of any records kept as a result of investigations.
PART 2 – Surveillance

2.1 Types of Surveillance

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

Covert Surveillance is surveillance that is carried out in a calculated manner to ensure that the persons subject to the surveillance are unaware that it is or may be taking place. Surveillance may be ‘directed’ or ‘intrusive’.

Local Authorities are NOT authorised to conduct Intrusive Surveillance, or to interfere with the property of others whilst conducting directed surveillance.

Intrusive Surveillance – is carried out in relation to anything taking place on any residential premises or in any private vehicle by an individual on the premises or in the vehicle or is carried out by means of a surveillance device, although a surveillance device not on or in the premises/vehicle will only be intrusive if it consistently provides information of the same quality and detail as might be expected to be obtained for a device actually on/in the premises/vehicle.

Directed Surveillance – surveillance is directed surveillance if the following are all true:

- it is covert, but not intrusive surveillance
- it is conducted for the purposes of a specific investigation or operation
- it is likely to result in the obtaining of private information about a person (whether or not one specifically identified for the purposes of the investigation or operation)
- it is conducted otherwise than by way of an immediate response to events or circumstances, the nature of which is such that it would not be reasonably practicable for an authorisation under RIPA to be sought.

Private Information:

For the purposes of RIPA includes any information relating to a person’s private or family life. Private information should be taken generally to include any aspect of a person’s private or personal relationship with others including family and professional or business relationships.

While a person may have a reduced expectation of privacy when in a public place, covert surveillance of that person’s activities in a public place may still result in the obtaining of private information.

Deciding when authorisation under RIPA is required involves making a judgement. The flowchart at Appendix 4 may help. Where surveillance is covert and is directed at individual(s) to obtain information about them, RIPA is likely to apply and prior authorisation from the Magistrates’ Court must be obtained in accordance with this document. If in doubt, seek authorisation.
2.2 Authorisation

Directed surveillance must be authorised in accordance with this policy and must only be used for investigating an offence which meets the statutory conditions, where it is necessary on one or more of the statutory grounds and is proportionate to what it seeks to achieve. It is extremely important that all reasonable alternative methods to resolve a situation, such as naked-eye observation, interview or changing methods of working or levels of security should be attempted first and recorded in writing and the reason for surveillance being requested is fully documented.

All requests to conduct, extend or discontinue a covert surveillance exercise must be made in writing on the Council's corporate forms, in accordance with Part 4 of this document, first to an Authorising Officer of the Council and thereafter to the Magistrates Court for Judicial approval. Authorisations for Directed Surveillance will be valid for 3 months from the date of the original authorisation or extension.

Authorising Officers are responsible for ensuring that surveillance is cancelled as soon as it is no longer required, and for ensuring that reviews of authorisation are carried out on at least a monthly basis. There is no requirement for judicial approval of internal reviews or cancellations.

There is no longer any scope for urgent authorisations to be approved orally. All authorisations must be judicially approved by a Magistrates’ Court.

Embarking upon Directed surveillance without authorisation or conducting Directed surveillance outside the scope of the authorisation will not only mean that the ‘protective umbrella’ of RIPA is unavailable but may result in disciplinary action being taken against the officers involved.

2.3 Equipment

Surveillance equipment will only be installed with the necessary authorisation of the Council’s Authorising Officers. Any permission to locate surveillance equipment in occupied residential premises must generally be obtained in writing from the owner, occupier or tenant.

Use of audio and photographic recording equipment which falls within the scope of the Act, for example, where a resident uses equipment provided by the Council to provide evidence to a council officer, may require authorisation. The Home Office Code of Practice for Covert Surveillance and Property Interference 2014 states that current recording of suspected noise nuisance where the intention is only to record excessive noise levels from adjoining premises and the recording device is calibrated to record only excessive noise levels does not constitute either directed or intrusive surveillance. This is on the grounds that the perpetrator would normally be regarded as having forfeited any claim to privacy and authorisation may not therefore be necessary.
2.4 Risk Assessments and Health & Safety

Although a risk assessment is unnecessary for the granting of an authorisation by an Authorising Officer, a risk assessment is required to be undertaken by an investigating officer prior to the commencement of an investigation. Officers should refer to the Council’s Risk Management page on the Council’s intranet and to the Council’s Health and Safety Policy.

2.5 Authorising Officers

The list of posts of Authorising Officer is shown at Appendix 1. Investigating Officers must seek authorisation from one of these Authorising Officers prior to submitting an application to the Magistrates' Court.

2.6 Evidence

During a covert operation, recorded material or information collected will be stored and transported securely. It will be reviewed regularly (at least weekly) and access to it will be restricted to the Head of Corporate and Customer Services, Authorising Officers and the investigating officers concerned. The Authorising Officers will decide whether to allow requests for access by third parties including council officers. Access will generally only be allowed to limited and prescribed parties including law enforcement agencies, prosecution agencies, legal representatives and the people subject to the surveillance (unless disclosure would prejudice any criminal enquiries or proceedings). Authorising Officers will maintain a record of all reviews of material recorded and collected covertly.

Only high quality digital equipment for audio and video recordings will be used. All recordings will be identified uniquely. A register will be kept of all recordings used to control the period of time they are retained, if not required for evidential purposes. In cases where an Interview under Caution has taken place, these types of records should be kept for at least two years from:

(a) The date the appropriate officer decides that criminal proceedings are inappropriate.
(b) Solicitors decide the case is not suitable for prosecution.
(c) A court dismisses a case.
(d) The defence or the prosecution withdraws a court case.
(e) A court case collapses.
(f) The file is closed when the question of recommending criminal proceedings does not arise.

In cases where an Interview under Caution has not taken place, records, material and information should be held for at least 6 weeks.

The holding or use of any material gathered during the course of an operation/investigation must comply with the provisions of the Data Protection Act 1998 and from the 25 May 2018, The General Data Protection Regulation 2016. Officers are referred to the Data Protection Act guide for employees on the Council’s intranet.
Once a covert operation confirms a suspicion of an individual having committed a criminal offence, he/she must be informed of this as promptly as is reasonably practicable if the relevant department is pursuing the offences internally. In all other cases the police will be informed to ensure an individual’s right to a fair trial or hearing within a reasonable time in accordance with the Human Rights Act. In a situation where it is considered that a matter gives rise to a potential criminal prosecution, any interview with the suspect must be ‘under caution’ and conducted by a suitably trained officer. If appropriate, the police will be involved immediately to ensure that evidential procedures and the requirements of current legislation are observed. Authorising Officers will note any recorded material handed over to the police.
PART 3 - Covert Human Intelligence Sources (CHIS)

3.1 Definition

A person is a CHIS if:

(a) he establishes or maintains a personal or other relationship with a person for the covert purpose of facilitating the doing of anything falling within paragraphs (b) or (c) below;

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

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

A CHIS may be required to establish or maintain a personal or other relationship for a covert purpose, i.e. one which the person with whom the relationship is established is unaware of. A CHIS is “tasked” to obtain information, provide access to information or to otherwise act, incidentally, for the benefit of the relevant public authority. Authorisation for the use or conduct of a CHIS is required prior to any tasking where such tasking requires the CHIS to establish or maintain a personal or other relationship for a covert purpose.

However, the provisions of the 2000 Act are not intended to apply in circumstances where members of the public volunteer information as part of their normal civic duties, or to contact numbers set up to receive information e.g. Crime stoppers or Anti-Fraud Hotline. Members of the public acting in this way would not generally be regarded as sources. A routine test purchase which does not go beyond a normal transaction is unlikely to be considered a CHIS activity.

The use of a CHIS by the Council is likely to be infrequent and it is not the Council’s normal practice to seek, cultivate or develop a relationship with a potential external or professional source. However the Council recognizes that there may be exceptional circumstances in which it is necessary to use a CHIS, and the procedures set out in this document must be followed if such circumstances arise.

A judgement must be made in determining when an individual taking part in an investigation may be acting as a CHIS and if officers are in any doubt, they should seek advice from Legal Services.

3.2 Authorisation

The same principles and procedures apply for the authorisation of a CHIS as for directed surveillance (see parts 2 & 4). The Authorising Officers listed in Appendix 1 may authorise applications for the use of a CHIS to proceed to the Magistrates’ Court for judicial approval, provided that they are satisfied that it is necessary and proportionate to do so and that there are arrangements in place (set out below) for managing a CHIS. Applications
involving confidential information or vulnerable persons or juveniles must be approved by the Chief Executive (see paragraphs 3.5 and 4.2). Use of a CHIS by the Council is only permitted if it is necessary for the prevention or detection of crime or the prevention of disorder. Applications to use or extend the use of a CHIS must be made in writing on the Council’s corporate forms, as set out in Part 4 and submitted to the Magistrates’ Court for approval. A CHIS will be valid for 12 months from the date of court approval. As with directed surveillance, authorising officers are responsible for ensuring that authorisation is cancelled as soon as it is no longer required, and that reviews of authorisations are carried out on at least a monthly basis.

There are additional considerations which must be taken into account before the use of a CHIS can be authorised. These relate to the security, welfare and management of the source and records relating to his/her use. Details of these issues are set out in paragraphs 3.3 – 3.5 below.

Material obtained from a CHIS may be used as evidence in criminal proceedings and the proper authorisation of a CHIS should ensure the legality of such evidence.

Before considering the use of a CHIS, the Authorising Officer and investigators must ensure that, as far as is possible, measures are taken to avoid unnecessary intrusion into the lives of those not directly connected with the investigation.

An authorisation for a CHIS may be in broad terms and highlight the nature of the CHIS’s task. However, where it is intended to task a source in a new or significantly greater way, the handler or controller (see below) must refer the proposed tasking to the Authorising Officer, who should consider whether a separate authorisation is required.

There is no longer scope for urgent authorisations to be approved orally as all authorisations must be approved by a Magistrates’ Court.

3.3 Management of the Source

An Authorising Officer must not approve an authorisation or associated application to the Magistrates’ Court for the use or conduct of a source unless he/she has appointed a person who is to be responsible for having day to day contact with the CHIS, and a person with the responsibility for the general oversight of the use of the CHIS.

The person with the general oversight of the CHIS will be a ‘Controller’.

The person with day to day responsibility will be a ‘Handler’ and will deal with the CHIS on behalf of the Council, direct the day to day activities of the CHIS, record the information supplied by him/her and monitor the security and welfare of the CHIS. Meetings with the source must be recorded, along with details of meetings between the source and the subject of the investigation. Where there are unforeseen occurrences, these should be recorded as soon as practicable after the event, and the authority checked to ensure that it covers the circumstances that have arisen.
3.4 Record Keeping

Proper records must be kept of the authorisation and use of a source.

The Regulation of Investigatory Powers (Source Records) Regulations 2000 (SI2000/2725) provides that the following records must be kept when a CHIS is authorised:

- The identity of the source
- The identity, where known, used by the source
- Any relevant investigating authority other than the authority maintaining the records
- The means by which the source is referred to within each relevant investigating authority
- Any other significant information connected with the security and welfare of the source
- Any confirmation made by a person granting or renewing an authorisation for the conduct or use of a source that relevant information has been considered and that any identified risks to the security and welfare of the source have where appropriate been properly explained to and understood by the source
- The date when, and the circumstances in which, the source was recruited,
- The identities of the persons who will act as handler, controller and person responsible for maintaining records of the use of the source
- The periods during which those persons have discharged those responsibilities
- The tasks given to the source and the demands made of him in relation to his activities as a source
- All contacts or communications between the source and the Council’s handler
- The information obtained by the Council by the conduct or use of the source
- Any dissemination by that authority of information obtained in that way
- Any payment benefit or reward made or provided to the source (other than where the source is a council employee acting as an undercover operative).

The Home Office Code of Practice on the use of CHIS also contains additional advice on records to be kept in relation to a source. In addition to the authorisation forms, risk assessment, and the above information, a record should be kept of the circumstances in which tasks were given to the source and the value of the source to the Council.

The records must be kept in a way that preserves the confidentiality of the source and the information provided by him/her. Records must not be made available to other officers unless it is necessary to do so. The Authorising Officer must not authorise the use of a CHIS until an appropriate officer has been designated as the person with responsibility for maintaining a record of the use made of the CHIS, and arrangements are in place for ensuring that the records will be kept securely.
3.5 Safety & Security

Prior to the authorising of a CHIS, the Authorising Officer shall have regard to the safety and welfare of the CHIS and shall continue to have such regard, throughout the use of the CHIS. The safety and welfare of the CHIS after the authorisation has been cancelled or where the investigation has been closed, must also be taken into account at the outset. Officers seeking authorisation to use a CHIS must complete the corporate risk assessment (available from the Council’s RIPA page on the Council’s intranet site) to determine the risk to the source of any tasking and the likely consequences should the role of the source become known and provide it to the Authorising Officer for consideration. The nature and magnitude of risk to the source must be identified and evaluated. Risk on a personal, operational and ethical basis must be considered. The risk assessment must be taken into account by the Authorising Officer in deciding whether it is appropriate for authorisation to be granted for the use of the CHIS, along with the usual considerations of proportionality, necessity etc. The Authorising Officer must satisfy himself that any risks identified are justified in relation to the investigation, and that any identified risks have been properly explained and understood by the source. A copy of the risk assessment must be kept in accordance with the preceding paragraph.

The handler of the CHIS will be responsible for bringing any concerns about the personal circumstances of the source to the attention of the controller, in so far as they may affect the validity of the risk assessment, the conduct of the source and the safety and welfare of the source. Where appropriate such concerns should be brought to the attention of the Authorising Officer and a decision taken on whether or not to allow the authorisation to continue.

The use of vulnerable individuals, such as the mentally impaired, for a CHIS purpose must only be authorised by the Chief Executive (or in his/her absence the Executive Director), and only in the most exceptional cases. Authorising Officers should also abide by the Home Office Code of Practice relating to juveniles. On no account should the use or conduct of a source under 16 years of age be authorised to give information where the relationship to which the use of the source relates is between the source and his parents or any person who has parental responsibility for him. In other cases authorisation should not be granted unless the special provisions contained within the Regulation of Investigatory Powers (Juveniles) Order 2000 (SI2000/2793) are satisfied. These requirements relate to the presence of an appropriate adult (e.g. a parent) at meetings with the source and consideration of risk assessments. Authorisation of a juvenile CHIS may only be granted by the Chief Executive (or in his/her absence the Executive Director) and the duration of such an authorisation will be only one month, rather than twelve months.
PART 4 - Requesting Authorisation to use Covert Surveillance & CHIS

4.1 Procedure

All requests for authorisation to undertake Covert Surveillance or use of a CHIS must be done via the corporate application forms which are available from the RIPA page of the Council’s intranet site. Appendix 3 to this policy contains guidance to Officers on completion of the application form for directed surveillance (RIPA1), but is also generally applicable to the completion of all other RIPA forms.

The investigator/applicant must have completed a Risk Assessment prior to submitting the Authorisation Request. The Risk Assessment must be submitted with the Authorisation Request.

All elements of the form must be completed with sufficient detail and justification to enable the Authorising Officer to make an informed decision. Prior to submitting the form to the Authorising Officer, the form will be checked by a Supervisor within the department of the investigator/applicant. Authorising Officers are responsible for nominating at least two Supervisors to perform this function in their departments. The Supervisor will check that the Application Form has been fully completed in accordance with the guidance contained in Appendix 3. If insufficient information/justification is provided, the Supervisor will refer the request back to the Investigating Officer for further details. The content of the application form must also be checked at this stage by the Council’s Legal Services section. The Authorising Officer must consider whether the proposed surveillance is justified, necessary and proportionate, and will only authorise the surveillance if he/she is satisfied on these points. If not, the Authorising Officer must refuse authorisation and the surveillance cannot proceed.

If the Authorising Officer approves the application the Applicant must then seek an Order from the Magistrates’ Court via the Council’s legal department and will need to attend Court to give oral evidence at a private hearing.

If the Magistrates’ Court refuses the application the surveillance cannot proceed.

4.2 Confidential Information and Role of Authorising Officers

The Authorising Officers 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, in a small organisation such as Wrexham County Borough Council, or where it is necessary to act urgently. Where an Authorising Officer authorises such an investigation or operation it must be noted on the Matrix Control Sheet. The Chief Executive (or in their absence the Executive Director) is required to authorise any activity when knowledge of confidential information (confidential personal information, legally privileged information and confidential journalistic material) is likely to be acquired.
4.3 Reviews, Renewals and Cancellations

Authorising Officers are responsible for ensuring that authorisations are reviewed on a monthly basis.

If the surveillance activity is longer than first thought, a renewal of the authorisation should be sought and a renewal application submitted to the Magistrates’ Court for approval prior to the expiry of the original authorisation.

In all cases authorised, a departmental Matrix Control Sheet should be completed.

If the surveillance activity is cancelled, a Cancellation Form must be completed. There must be a cancellation form for each authorisation as soon as the requirement for surveillance ceases.

All forms (authorisations, refusals, reviews, renewals and cancellations) must be provided to the Head of Corporate and Customer Services, to include in the Central Record (see below).
PART 5 - Central Record

The Head of Corporate and Customer Services will maintain a register (with unique reference numbering) of all requests and authorisations for covert surveillance together with reasons for any request being denied. The records in this central register will be kept for three years. A copy of each RIPA form is kept along with a register of the details for each authorisation and Magistrates’ Court Order including date and type of authorisation, subject of surveillance, identity of Authorising Officer and dates of reviews, cancellations and renewals. The Central Record will be reconciled with departmental RIPA matrix control sheets on a three monthly basis.

The Head of Corporate and Customer Services must be notified by email that a RIPA form is to be sent to the Central Record, by way of the RIPA receipt form available from the RIPA page of the Council’s intranet site.

All RIPA forms must be sent to Legal Services within 2 working days of authorisation being granted or refused. The receipt of the RIPA form will be acknowledged by email.

The Council’s Head of Corporate and Customer Services will be responsible for monitoring authorisations and carrying out an annual review of applications, authorisations, refusals, extensions and cancellations, based on the information contained in the Central Record. RIPA forms will be checked for quality on receipt of forms for the Central Record by Legal Services staff, on a random selection basis.
PART 6 - Requests for Council Officers to undertake Covert Surveillance

The CCTV Control Room staff may be requested to undertake covert surveillance on behalf of other organisations such as the Police, or other departments. Such requests must be supported by an appropriate RIPA Authorisation from the relevant department or organisation together with the relevant Magistrates’ Court Order (if required) and directed to the Council’s Facilities Management Lead.
7.1 Introduction and Types of Communications Data

The Order permits access to communications data by local authorities only where it is necessary for the prevention or detection of crime or the prevention of disorder. As with surveillance, access to communications data should only be authorised where it is proportionate to the objectives the Council is seeking to achieve i.e. it should not be authorised where less intrusive means can be used to further an investigation.

The Order only permits local authorities to gain access to two types of communications data:

Service Data – this is information held by a telecom or postal service provider about the use made of a service by a person under investigation e.g. itemised telephone bills/outgoing call data.

Subscriber Data – any other information or account details that a telecom/postal service provider holds on a person under investigation.

Local Authorities are NOT authorised to obtain access to “traffic data” i.e. information about when communications were made, who from and who to. Further, these powers do not permit access to the contents of the communication itself.

All requests to obtain communications data must be made via The National Anti-Fraud Network. Authorisation will only be granted where access to communications data deemed to be necessary and proportionate and a Magistrates’ Court Order will also be required.

7.2 Designated Persons

The Order refers to persons who may authorise the acquisition of communications data as ‘designated persons’. The posts listed in Appendix 2 are authorised by the Council to act as designated persons for the purposes of the Order.

7.3 Single Point of Contact (SPOC)

The Home Office Code of Practice recommends that all authorities who use these powers appoint a SPOC who is to:

- assess whether it is reasonably practicable to obtain the communications data requested,
- advise applicants/authorising officers on the types of communications data that can be obtained;
- check that the Form is properly completed and authorised; and
- liaise with the service providers on obtaining the communications data requested.

All SPOC’s must attend an accredited course and obtain a PIN reference from the Home Office before they may act as a SPOC. The PIN reference number is given to the service provider with each request for data, so that the service
provider can be sure that they are providing the data to a properly accredited and authorised person within the Authority.

The Council is a member of the National Anti-Fraud Network (NAFN) and NAFN currently undertakes the role of SPOC for the Council. All requests for Communications Data should be directed to NAFN.

7.4 Procedure

The Order permits access to communications via an ‘authorisation’ under section 22(3) of RIPA or a ‘Notice’ under Section 22(4) which has been judicially approved by the Magistrates Court.

All applications for communications data will be via NAFN. The investigator/applicant must first be registered with NAFN and if an officer/applicant is not so registered he/she should in the first instance speak with their Line Manager who in turn will discuss with one of the designated persons or the Legal, Democratic and Registration Services Manager.

The investigator/applicant will submit the application on the NAFN website, the allocated SPOC at NAFN will check for legal compliance and where necessary provide feedback before submitting for approval from a designated person.

Following approval by the designated person the SPOC at NAFN will prepare a court pack which will be submitted to the investigator/applicant who will liaise with the Council’s Legal Services Section to seek judicial approval by the Magistrates Court.

If judicial approval is obtained, the Order should be returned to NAFN who will then obtain the data requested.

If judicial approval is not forthcoming the investigator/applicant must inform NAFN who will not be able to obtain the relevant communications data but may be able to assist in preparing a fresh application for consideration.

All aspects of administration are covered by NAFN including the tracking of reportable/recordable errors, cancellation, and withdrawals.

Applicants and designated persons must be aware that any information obtained as a result of these powers is likely to be ‘personal data’ within the meaning of the Data Protection Act 1998. Therefore, the requirements of the Data Protection Act 1998 and its principles must be adhered to in respect of this data.

Oral applications for communications data are not permitted.

7.5 Errors

The SPOC (NAFN) will record any errors that occur during acquisition of communications data. Such errors will be reported to the Interception of Communications Commissioner’s Office.
PART 8 – Surveillance by Use of Social Media

Regarding the gathering of evidence by surveillance through the use of Social Media, Officers must refer to the Council’s RIPA SNS guidance document and to the Council’s Social Media Policy.
PART 9 - Complaints

Any person who reasonably believes that they have been adversely affected by any activities carried out pursuant to this policy by or on behalf of the Council may complain to the Head of Corporate and Customer Services who will investigate the complaint. Such a person may also complain to the Investigatory Powers Tribunal at:-

Investigatory Powers Tribunal
PO Box 33220
London, SW1H 9ZQ

Tel: 0207 035 3711
Website: http://www.ipt-uk.com
APPENDIX 1

LIST OF AUTHORISING OFFICER POSTS

1. Chief Executive
2. Executive Director (with responsibility for this function)
3. Head of Environment and Planning
4. Public Protection Service Manager

APPENDIX 2

SINGLE POINT OF CONTACT

National Anti-Fraud Network (NAFN)

LIST OF DESIGNATED PERSON POSTS

1. Executive Director (with responsibility for the function).
2. Head of Corporate and Customer Services
3. Head of Environment and Planning
4. Public Protection Service Manager
GUIDANCE TO STAFF – COMPLETION OF RIPA1 FORM
APPLICATION FOR AUTHORISATION TO CARRY OUT DIRECTED SURVEILLANCE

Forms

A set of Wrexham County Borough Council RIPA forms is available on the Council’s Intranet.

This note contains guidance on the completion of the RIPA1 Form (Application), by reference to page and box numbers on the form. However the guidance is also generally applicable to completion of the other RIPA forms, which must similarly include as much detail/information as possible.

Page 1

1 Insert the unique reference number of the application in the box at the top right-hand corner of the page. This number will be the next available number from the Central Record, for the Department/Section applying for the authorisation. The Central Record is held by the Head of Corporate and Customer Services and the next number can be obtained by telephoning the Legal, Democratic and Registration Services Manager on 292221. The unique reference number (URN) must be inserted in the box on each page of the form.

2 The Investigating Officer should insert his/her name in the box in the middle of page 1, along with his/her department and section, address and contact details. The Investigating Officer should also allocate a name for the investigation/operation and insert this in the appropriate box on page 1. If the Investigating Officer is a person other than the applicant for the surveillance then the name of the Investigating Officer should go in the box provided in page 1.

3 Box 1 - Title of Authorising Officer. Insert the title of the Authorising Officer who is to be asked to authorise the surveillance. Please note that only those Officers whose title appears at Appendix 1 of the Council’s RIPA policy are authorised by the Council to act as Authorising Officers under RIPA. There are currently four Authorising Officers.

Page 2

4 Box 2 - Purpose of the operation/investigation. The Investigating Officer must include a full, clear explanation of the nature of the investigation or operation, and the intelligence/information that has led to it being instigated. Sufficient information must be given in this box to enable the Authorising Officer to gain a full understanding of the need for the surveillance and the background to the matter. Sufficient information should be included to allow the Authorising Officer to gain this understanding without a need to see the departmental file on the matter.

5 Box 3 - Description of the surveillance. Similarly in this box, the Investigating Officer must include a full description of the surveillance which is to be carried out. Examples of information to include are:-
• Whether the surveillance is static or mobile (i.e. from a property or vehicle).
• What the focus of the surveillance is, i.e. on a property (give address) or car (give registration number, make and colour).
• The expected duration of the surveillance including targeted hours. If the surveillance is unlikely to be 24 hours a day then the application for authority to carry out the surveillance should be limited to the times of day during which surveillance will be likely to take place.
• Where appropriate, attach a map showing the location of the surveillance with relevant points identified on it.
• Describe the type of equipment to be used (eg handheld camera with zoom lens). Applications in respect of noise nuisance monitoring should be explicit regarding the technical capability of the recording equipment.

6 **Box 4 - Identities of subjects.** Where known, the name, address and date of birth of the subjects of the surveillance should be inserted in Box 4. If these details are unknown, this should be stated. Any other information relevant to the identity of the subject should be included.

7 **Box 5 - Desired result.** State here what you are hoping to achieve by carrying out the surveillance, i.e. what is the objective of it? For example, to obtain photographic evidence that the subject is employed or to establish that the subject is selling counterfeit goods.

Page 3

8 **Box 6 - Grounds.** The only ground on which Local Authorities may carry out directed surveillance is for the purpose of preventing or detecting crime or preventing disorder and the offence under investigation is either:-

• An offence attracting a penalty of at least six months imprisonment; or

• An offence contrary to:
  
  i) Section 146/147/147A of the Licensing Act 2003; or
  ii) Section 7 of the Children and Young Persons Act 1993

Insert details of the offence under investigation in this box.

9 **Box 7 - Necessity.** This box requires an explanation of why directed surveillance is necessary in this case. As a pre-requisite, Investigating Officers should always consider and try to resolve the situation via a less intrusive means than surveillance, e.g. interviewing subject. Only where it is the only means of obtaining evidence will surveillance be necessary within the requirements of the RIPA Act. This therefore needs to be explained by the Investigating Officer in this box, in respect of the particular application. The following information should be included:-

• Briefly reiterate the background to the investigation, including the offence which is being investigated.
• Provide details of alternative attempts to resolve the situation which have proved unsuccessful.
• Explain why covert surveillance is necessary in order to prevent or detect the particular crime or disorder concerned.
• Explain what the likely effect will be if overt surveillance is carried out (eg destruction of evidence by suspect).

10 **Box 8 - Collateral intrusion.** Collateral intrusion is the term used to describe the risk of obtaining private information about persons other than the subject of the surveillance. This is likely to affect friends, family, neighbours etc. of the subject. Investigating Officers must plan the surveillance in a way which assesses the risk of collateral intrusion and details of any measures taken to limit this should appear in this box. Details to include are:-

• Identifying who is at risk of collateral intrusion (being unintentionally included in the surveillance) e.g. friends, family, neighbours, colleagues and staff of subject, and members of the public.
• Identify how this risk of intrusion will be minimised, e.g. by targeting the cameras on a specific entrance to a premises/vehicle which is only used by the subject.

Page 4

11 **Box 9 – Proportionality.** Proportionality is a key concept of RIPA. An authorisation should demonstrate how an Authorising Officer has reached the conclusion that the activity is proportionate to what it seeks to achieve including an explanation of the reasons why the method or tactic proposed is not disproportionate.

Each action authorised should bring an expected benefit to the investigation and should not be disproportionate or arbitrary.

Proportionality is not only about balancing the effectiveness of covert methods over overt methods but of explaining why the particular covert method, is the least intrusive.

No activity should be considered proportionate if the information which is sought could reasonably be obtained by other less intrusive means, or if it is excessive compared with the seriousness of the crime suspected.

A model authorisation would make it clear that the four elements of proportionality had been fully considered:

• balancing the size and scope of the operation against the gravity and extent of the perceived crime or disorder
• explaining how and why the methods to be adopted will cause the least possible intrusion on the target and others
• that the activity is an appropriate use of the legislation and the only reasonable way, having considered all others, of obtaining the necessary result, and
• evidencing what other methods have been considered and why they were not implemented.

12 **Box 10 - Confidential information.** This box requires an assessment of whether the following types of information may be acquired through surveillance:-

• Legal communications between lawyer and client.
• Confidential personal information, e.g. communication between a doctor and patient, social worker and client, or priest and parishioner.

• Confidential journalistic material which includes material acquired or created for the purposes of journalism and held subject to an undertaking to hold it in confidence, as well as communications relating in information being acquired for the purposes of journalism and held subject to such an undertaking.

• Confidential constituent information – Information relating to communications between a Member of Parliament and a constituent in respect of constituency matters. Such information is held in confidence if it is held subject to an express or implied undertaking to hold it in confidence or it is subject to a restriction on disclosure contained in existing legislation.

If the assessment reveals that this type of material may be acquired by the surveillance, **then only the Chief Executive can authorise the acquisition of confidential information**. Investigating Officers should record their assessment in this box, giving reasons, and approach the Chief Executive for authorisation if it is considered that such material may be obtained, e.g. if the subject of the surveillance is a solicitor, doctor or journalist etc, or if the subject has substantial dealings with such persons which will be subject to the surveillance. Where such material will be obtained, this box should explain how its confidential nature will be protected, e.g. security arrangements/arrangements for destruction.

Advice should be sought from Legal Services before applying for authorisation where there is any doubt as to whether such information may be acquired.

13 **Box 11 - Applicant’s details.** The Investigating Officer should insert his/her name, title and telephone and sign and date in this box.

Page 5

14 **Box 12 - Authorising Officer’s statement.** Following consideration of the information given in the previous boxes, if the Authorising Officer is satisfied that the proposed surveillance is necessary and proportionate, he/she must record this fact in this box and also in Box 13 (see below). As indicated on the form, the Authorising Officer should spell out the five W’s - Who, What, Where, When, Why and How. The Authorising Officer should set out why the surveillance is necessary, who the surveillance is directed against, where and when it will take place and what surveillance activity/equipment is sanctioned. The Authorising Officer should also explain how it is to be achieved. Authorisations for noise nuisance monitoring should explicitly describe the nature of the noise being recorded and the circumstances of it.

For the benefit of those operating under the terms of an authorisation or any person who may subsequently review or inspect an authorisation it is essential that the statement is clear and states in the Authorising Officer’s own words explicitly what is being authorised. Mere reference to the terms of the application is inadequate.

If an application fails to include an element in the proposed activity that, in the opinion of the Authorising Officer, should be included or which is subsequently
requested orally by the Applicant, it may be included in the Authorisation. If it is a note should be added explaining why.

Conversely, if an Authorising Officer does not authorise all that is requested, a note should be added explaining why.

The Authorising Officer must be careful in the use of ‘or’ and ‘and’ in order not to restrict what is intended, e.g. do not use ‘or’ when ‘and’ is meant (e.g. ‘deployment of on Vehicle A or Vehicle B’ limits deployment to either vehicle, not both simultaneously or one after the other).

**Box 13 - Explanation of necessity and proportionality.** In this box the Authorising Officer should record why he/she considers the surveillance necessary and proportionate. Although this may seem repetitive it records exactly what activity is authorised and shows that the Authorising Officer has properly considered the issues of necessity and proportionality.

**Page 6**

**Box 14 - Confidential information authorisation.** If it is considered that confidential information may be acquired during the surveillance, then if the Chief Executive considers that the surveillance should be authorised, Box 14 should be completed by the Chief Executive providing the same information as required in Boxes 12 and 13.

**Date of Review** - The date of the first review of the authorisation should be inserted in the relevant box on this page by the Authorising Officer, together with a programme of the subsequent reviews.

**Signature of Authorising Officer** - If the Authorising Officer is satisfied that the surveillance should be authorised, following completion of Boxes 12, 13 and 14 (if appropriate) the Authorising Officer should complete the details in the box at the bottom of page 6 providing their name, title and date and time authorised and signing in the relevant box. The Authorising Officer should also complete the box which requires the expiry date and time of the authorisation to be completed. Authorisations for directed surveillance have a duration of three months and the appropriate date and time should be inserted in this box.

**Page 7**

**Box 15 - Urgent Authorisation.** This box does not apply as all applications must be approved by order of the Magistrates’ Court.

**Box 16 - Urgent Authorisations - Non Authorising Officers.** This box does not apply to local authorities since only the designated Authorising Officers can authorise urgent application in local authorities. If the departmental Authorising Officer is not available to authorise an urgent application, the investigating officer may approach any of the other Authorising Officers listed in Appendix 1 of the Council’s RIPA Policy.

Following completion of the application form by the investigating officer and Authorising Officer, the advice of the of the Legal Services section regarding the content of the application must be obtained.
Application for Judicial Approval

All applications pursuant to RIPA must now be approved by order of the Magistrates’ Court. This form must be completed following approval by the Authorised Officer and the Legal services section and then arrangements made via the Legal services section for a private hearing at the Magistrates’ Court for judicial approval.
Appendix 4  RIPA 2000 - Do you need Authorisation?

Are you carrying out an investigation?

YES

Is it Covert?

YES

Does it involve a person establishing or maintaining a personal or other relationship with the covert purpose of facilitating:

- The covert use of the relationship to gain information or
- The covert use of the relationship to provide access to information to another person or
- To covertly disclose information obtained by the use of the relationship or as a consequence of its existence.

NO

RIPA does not apply

NO

Are you carrying out an investigation?

YES

Is it specific to an investigation/operation?

YES

NO

Is it Covert?

YES

NO

Is it likely to result in private information being obtained about a person?

YES

NO

Not Directed Surveillance -

NO

Yes

Is it an immediate response to events and impracticable to obtain authorisation?

YES

RIPA authorisation not required

NO

INTRUSIVE SURVEILLANCE - NOT PERMITTED

Seek legal advice.

Not Intrusive Surveillance

COVERT HUMAN INTELLIGENCE SOURCE

Authorisation required.

Not Covert Human Intelligence Source

DIRECTED SURVEILLANCE (unless it is Intrusive Surveillance)

Authorisation required.