### Document Change Control

<table>
<thead>
<tr>
<th>Version Number</th>
<th>Date Approved</th>
<th>Reason for change</th>
<th>Issued by</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.0 (draft)</td>
<td>N/A</td>
<td>Draft policy – review</td>
<td>N/A</td>
</tr>
<tr>
<td>2.0 (draft)</td>
<td>N/A</td>
<td>Draft policy – final draft</td>
<td>N/A</td>
</tr>
<tr>
<td>3.0 (final)</td>
<td>Jul06</td>
<td>Finalised policy</td>
<td>N/A</td>
</tr>
<tr>
<td>4.0</td>
<td>Oct07</td>
<td>Content reviewed and simplified &amp; Application Forms updated</td>
<td>KJM</td>
</tr>
<tr>
<td>5.0</td>
<td>Apr08</td>
<td>General Review &amp; Authorising Officers Updated</td>
<td>KJM</td>
</tr>
<tr>
<td>6.0</td>
<td>Nov08</td>
<td>Additions as per OSC Inspector’s Recommendations following Jun08 Inspection; Amendments to reflect Council internal changes</td>
<td>KJM</td>
</tr>
<tr>
<td>7.0</td>
<td>May09</td>
<td>Revision of contact details for Devon Audit Partnership</td>
<td>KJM</td>
</tr>
<tr>
<td>8.0</td>
<td>Mar11</td>
<td>Update of RIPPA</td>
<td>KP</td>
</tr>
<tr>
<td>9.0</td>
<td>Jul11</td>
<td>Additions as per OSC Inspector’s Recommendations following Apr11 inspection</td>
<td>KP</td>
</tr>
<tr>
<td>10.0</td>
<td>Jul12</td>
<td>Update to authorising officers</td>
<td>KP</td>
</tr>
<tr>
<td>11.0</td>
<td>Apr 13</td>
<td>To take into account changes involving Magistrates approval. Change of details</td>
<td>KP</td>
</tr>
<tr>
<td>11.1</td>
<td>Apr14</td>
<td>Review ready for committee</td>
<td>KP</td>
</tr>
<tr>
<td>12.0</td>
<td>Aug15</td>
<td>To encompass recommendations following June 2014 Inspection</td>
<td>KP</td>
</tr>
<tr>
<td>13</td>
<td>Jun 17</td>
<td>Bi-Annual review and update following updated OSC guidance</td>
<td>JB</td>
</tr>
</tbody>
</table>

**For advice and assistance contact**

Jo Beer
Corporate Support Manager
Telephone (01803) 207894
[Joanne.beer@torbay.gov.uk](mailto:Joanne.beer@torbay.gov.uk) or [infocompliance@torbay.gov.uk](mailto:infocompliance@torbay.gov.uk)

**Acknowledgements**

City of Nottingham Council
Redcar and Cleveland Borough Council
Basingstoke and Deane Borough Council

**Legislation referred to:**

- Human Rights Act 1998
- Data Protection Act 1998
- Police and Criminal Evidence Act 1984
Contents

1. INTRODUCTION ...........................................................................................................3
2. DEFINITIONS ..................................................................................................................6
3. DOES RIPA APPLY TO MY SITUATION? .................................................................12
4. AUTHORISATION PROCEDURES ...........................................................................14
5. URGENT AUTHORISATIONS ..................................................................................17
6. DURATION OF AUTHORISATIONS ..........................................................................17
7. MATERIAL OBTAINED DURING INVESTIGATIONS ...........................................18
8. ASSESSMENT AND REVIEW .....................................................................................19
9. CCTV AND DIRECTED SURVEILLANCE ...............................................................20
10. RECORDS MANAGEMENT .......................................................................................20
11. TRAINING ..................................................................................................................21

Appendices

1) Torbay Council RIPA Management Structure
2) Flowchart 1 – Are you conducting Directed Surveillance?
3) Flowchart 2 – Are you doing Intrusive Surveillance?
4) Flowchart 3 – Are you deploying a CHIS?
5) Flowchart 4 – Authorising Directed Surveillance
6) Flowchart 5 – Authorising a CHIS
7) Flowchart 6 – The Magistrates’ Approval Process
1. **INTRODUCTION**

1.1 The Regulation of Investigatory Powers Act 2000 (‘RIPA’) regulates covert surveillance activities undertaken by all public authorities. By following the procedures set out in the Act and in this Manual, Council employees can best ensure that any investigations they undertake as part of their work are lawful and do not constitute a breach of people’s human rights. It is important to emphasise that **RIPA only regulates surveillance that is ‘covert’** i.e. where employees do not want the targeted person to know that they are under surveillance.

1.2 The need to regulate the conduct of covert surveillance stems from the Human Rights Act 1998. Article 8 of the Human Rights Act gives people the right to respect for a private and family life and part of this includes the right not to be subject to unlawful surveillance by ‘The State’. As a local authority, the Council is part of ‘the State’ and ‘covert surveillance’ by Council employees may amount to an interference with a person’s right to respect for their person’s private life.

1.3 The Article 8 right to respect for private and family life is not an ‘absolute’ right. It is a ‘qualified’ right and may be overridden ‘in accordance with the law and is necessary in a democratic society’ on certain grounds.

1.4 Where authorised, RIPA provides lawful authority for covert surveillance by local authorities, however this is subject to various robust safeguards. If covert surveillance is authorised and undertaken in accordance with RIPA the Council will be able to argue that it has acted lawfully and not contravened the observed person’s human rights.

1.5 **Local authorities may only undertake covert surveillance for the purpose of ‘preventing or detecting crime or of preventing disorder’**. The ‘prevention of disorder’ must now comply with the Protection of Freedoms Act 2012 which demands an enhanced threshold test i.e. a penalty of six months or more imprisonment on first conviction, or related to the underage sale of alcohol or tobacco on those considering the use of RIPA powers. In relation to the ‘prevention of disorder’, this is unlikely to be achieved.

1.6 Investigation activities that are covered by RIPA are:

- Directed Surveillance
- Intrusive Surveillance
- Covert Human Intelligence Source (CHIS), and
- Acquisition of communications data.

1.7 **It must be noted, that the Council does not, under any circumstances, have the power to undertake ‘Intrusive Surveillance’. It is also the case that the Council cannot authorise the ‘interference with property’.** It may be the case that a Council officer may need to trespass onto land belonging to another without
consent during their duties, for example to deploy a covert camera. It is important that urgent advice is sought from Legal services in respect of such matters as there may be a 'civil' tort liability.

1.8 Employees within each Business Unit of the Council may, on occasion, need to conduct covert surveillance activities that will fall within the remit of RIPA where they will be obtaining information about a person without that person’s knowledge. Employees must ensure that they understand the meaning of ‘surveillance’ and obtain the appropriate authorisation before undertaking any covert surveillance.

1.9 The purpose of this guidance is to:

• explain the scope of RIPA and the circumstances where it applies
• provide guidance on the authorisation procedures which must be followed.

1.10 The flow charts in the appendices provide should assist officers in identifying whether RIPA applies.

1.11 The senior officers, as identified in Appendix 1, are all responsible for ensuring that applications for directed surveillance or the use of a CHIS are authorised appropriately.

1.12 Only those officers listed in Appendix 1, known as ‘Authorising Officers, may authorise Council employees to undertake covert surveillance.

1.13 The Authorising Officers listed in Appendix 1 must be sufficiently removed from the investigation that s/he can be deemed to manage it but are not involved in its day to day conduct. The Authorising Officer must not take part in the surveillance to which the application relates.

1.14 Only the relevant officers identified in Appendix 1 may authorise the use of a Covert Human Intelligence Source. The Authorising Officer must not take part in the surveillance or in the management of the Covert Human Intelligence Source to which the application relates.

1.15 Under normal circumstances, Authorising Officers will authorise activity within their own service area. If the relevant Authorising Officer is not available, or if there is a need to ensure / demonstrate an additional level of impartiality, than an Authorising Officer from a different business unit may be approached. Where more than one service area is involved the authorisation must be delegated upward through the RIPA management structure outlined in appendix one.

1.16 Details of the proposed surveillance must be shown on the authorisation forms. In the case of a Covert Human Intelligence Source, a risk assessment must be carried out which must accompany the authority form.
1.17 Before approving applications, the Authorising Officer must have regard to the necessity, proportionality and subsidiarity elements of the application (see paragraph 4.1.1) and record these on the forms. It is also important that any officers engaged on any surveillance, read all necessary information and certify that they have done so.

1.18 It is essential to remember that once obtained, the authorisation helps to protect the Council and its employees from complaints of unlawful interference with the human rights of the persons targeted by the covert surveillance.

1.19 There are Home Office codes of practice that expand on the information in this guide and copies are available on the Council’s Intranet, within the Information Governance pages, under the RIPA section.

The codes of practice are regarded as ‘secondary legislation’ as referred to in section 71 and 72 of the 2000 Act. As stated in the codes, ‘if any provision of the code appears relevant to a question before any Court or tribunal considering any such proceedings, or to the tribunal established under RIPA, or to one of the commissioners responsible for overseeing the powers conferred by RIPA, it must be taken into account’.

Staff must refer to the Home Office Codes of Conduct for supplementary guidance.

Deciding when authorisation is required involves making a judgment. The flowcharts in the appendices show how authorisations can be undertaken.

1.20 If you are unclear about any aspect of the process, seek the advice of an Authorising Officer. If they are unable to answer your questions they must seek advice from the contacts detailed above.

1.21 If you are in any doubt about whether a course of action requires an authorisation, seek advice from the appropriate Authorising Officer. If you are unable to secure an authorisation it is likely that your application does not comply with the law.

1.22 In the event that a particular Service Area of the Council that undertakes surveillance that is covered by RIPA may wish to develop specific guidance on the applicability of RIPA to their particular circumstances, the relevant Business Unit Manager must ensure that any ‘local’ guidance does not conflict with this corporate document.
2. DEFINITIONS

2.1 Surveillance includes:

- monitoring, observing or listening to persons, watching or following their movements, listening to their conversations or their other activities or communications.
- recording anything mentioned above in the course of authorized surveillance.
- Surveillance by, or with the assistance of, appropriate surveillance devices.

For the purposes of RIPA, the term ‘persons’ includes ‘any organisation and any association or combination of persons’, this will include companies, partnerships, co-operatives etc.

2.2 Covert Surveillance

Covert surveillance is any surveillance that is carried out in a manner calculated to ensure that the person/s subject to surveillance is/are unaware that it is or may be taking place.

2.3 Directed Surveillance is surveillance which:

- Is covert, and
- Is not intrusive surveillance (see definition in 2.4 below – the council is prohibited by law from carrying out intrusive surveillance)
- Is not carried out as an immediate response to events where it would not be practicable to obtain authorization under the Act,
- Is undertaken for the purpose of a specific investigation or operation in a manner likely to obtain private information about an individual (whether that person is specifically targeted for purposes of an investigation) (Section 26 (10) of RIPA).

2.4 Intrusive Surveillance occurs when surveillance is:

- Is covert,
- Relates to residential premises and / or private vehicles, and
- Involves the presence of a person in the premises or in the vehicle or carried out by a surveillance device in the premises/vehicle. It must be noted that surveillance devices / equipment mounted outside the premises will not be intrusive, unless the device consistently provides information of the same quality and details as might be expected is they were in the premises / vehicle.

NOTE: THE COUNCIL DOES NOT, UNDER ANY CIRCUMSTANCES, HAVE THE POWER TO UNDERTAKE ‘INTRUSIVE SURVEILLANCE’ THIS IS ALSO THE CASE FOR ‘INTERFERENCE WITH PROPERTY’ (see para 1.7)
2.5 **Covert Human Intelligence Source (CHIS)**

A person is called a Covert Human Intelligence Source if:

a) the source establishes or maintains a personal or other relationship with a person for the covert purpose of facilitating the doing of anything falling within paragraph b) or c) below.

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

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

The use of a CHIS requires authorisation under RIPA, but it considered unlikely that there will be a circumstance under which the council would use a CHIS or operate under cover, therefore advice should be sought from the RIPA monitoring officer or the Senior Responsible Office before any authorisation is applied for.

2.6 **Covert Purpose**

A purpose is covert, in relation to the establishment or maintenance of a personal or other relationship only if the relationship is conducted in a manner that is calculated to ensure that one of the parties to the relationship is unaware of the purpose behind the relationship.

2.7 **Private Information**

Private information is any information relating to a person’s (see the definition of person in 2.1 above) private or family life. For example, if part of an investigation is to observe a member of staff's home to determine their comings and goings then this surveillance would, almost certainly, gather private information, as would surveillance of an individual selling counterfeit goods, as the surveillance may provide information about the earnings that the person made from the sales.

2.8 **Confidential Material**

The term 'confidential material' includes:

a) matters subject to legal privilege
b) confidential personal information
c) confidential journalistic material
a) Matters Subject to Legal Privilege

Matters subject to legal privilege includes both oral and written communications between a professional legal adviser and his/her client (or any person representing his/her client) made in connection with the giving of legal advice to the client or in contemplation of legal proceedings and for the purposes of such proceedings, as well as items enclosed with or referred to in such communications.

Communications and items held with the intention of furthering a criminal purpose are not matters subject to legal privilege.

Legally privileged communications will lose their protection if there is evidence, for example, that the professional legal adviser is intending to hold or use them for a criminal purpose; privilege is not lost if a professional legal adviser is properly advising a person who is suspected of having committed a criminal offence. The concept of legal privilege shall apply to the provision of professional legal advice by any agency or organisation.

b) Confidential Personal Information

This is information held in confidence concerning an individual (whether living or dead) who can be identified from it, and relating:

• to his/her physical or mental health; or
• to spiritual counselling or other assistance given or to be given,
• and which a person has acquired or created in the course of any trade, business, profession or other occupation, or for the purposes of any paid or unpaid office

Confidential personal information might, for example, include consultations between a health professional or a professional counsellor and a patient or client, or information from a patient’s medical records.

It includes both oral and written information and also communications as a result of which personal information is acquired or created. 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 or an obligation of secrecy contained in existing or future legislation.

c) Confidential Journalistic Material

This 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
resulting in information being acquired for the purposes of journalism and held subject to such an undertaking.

Confidential material is not afforded any special protection by RIPA but is the subject of special safeguards under this code. The general principles that apply in handling confidential information are specified at section 4.4.4 of this guidance.

2.9 Residential Premises

These are premises / or part of premises which are occupied or used by any person however temporarily for residential purposes or otherwise as living accommodation (including hotel or prison accommodation). It does not include common areas e.g. hallways.

2.10 Private Vehicle

Any vehicle used primarily for the private purposes of the person who owns it or of a person otherwise having the right to use it (unless that right derives only from him having paid or undertaken to pay for the use of the vehicle and its driver for a particular journey).

2.11 Surveillance Device

Any apparatus designed or adapted for use in surveillance.

2.12 Communications Data

Chapter II of Part I of RIPA allows Local Authorities to access / acquire communications data for the purposes of preventing and detecting crime. The data accessible relates to subscriber details for telephones, mobile telephones, and internet / email and itemised billing information.

All requests for access to such data have to be authorised by the appropriate officer for RIPA authorisations and the acquisition of communications data is now undertaken by National Anti-Fraud Network who acts as the Single Point of Contact (SPoC) for all Communications Data requests.

This process is subject to a separate policy and procedures and therefore is not the subject of this policy.

2.13 Monitoring of Computer Usage

The Council has an agreed Information Security Framework which contains separate policies that govern the use of internet and email by staff. This also
contains details of the monitoring currently applied to internet and email use, and
the process for accessing an individual's internet history / log and emails.

2.14 **Necessity**

A RIPA authorisation may only be granted if the authorising officer believes that the conduct is **necessary** for one or more of the statutory purposes as specified in s28(3) of RIPA and s.29(3) of RIP(S)A. The statutory purposes in RIPA mirror the legitimate aims in Article 8 of the Human Rights Act. The RIPA Orders provide that local authorities may only authorise the use of covert techniques for the purpose of ‘the prevention and detection of crime or the prevention of disorder Preventing and detecting crime goes beyond the prosecution of offenders and includes actions taken to avert, end or disrupt the commission of criminal offences. The local authority must be satisfied that there is an identifiable offence to detect or prevent before authorising the use of any covert technique under RIPA. An explanation supporting the authorisation is required outlining why it is necessary to use the covert techniques requested. (note 72 OSC Procedures and Guidance 2016)

2.15 **Proportionality**

The authorising officer must also believe that the authorised conduct is proportionate to what it seeks to achieve. This involves balancing the seriousness of the intrusion into the privacy of the person under investigation against the need for the activity in investigative terms. If overt investigative methods would be effective, it is unlikely that covert activity will be proportionate and thus authorised.

The Authorising Officer also needs to ensure they take into account the risk of collateral instruction, which is the risk of intrusion into the privacy of persons other than those who are directly the subjects of the investigation.

Authorisation should demonstrate how the Authorising Officer has reached the conclusion that the activity is proportionate, including an explanation of the reasons why the method, tactic or technique proposed is not disproportionate.

A model investigation would include consideration of why the methods adopted would include the least possible intrusion to the subjects, alongside how appropriate use of the legislation was used. Finally providing evidence of other methods considered and why they were not implemented. (note 73 and 74 of the OSC Procedures and Guidance 2016).

2.16 **Internet and Social networking sites**

The Chief Surveillance Commissioner has made specific reference to the increasing use of social networking sites as a method of gathering intelligence. The
OSC Procedures and Guidance document, issued in July 2016, contains the following advice:

**Note 289 of the OSC's 2016 Procedures & Guidance document:**

289. **The fact that digital investigation is routine or easy to conduct does not reduce the need for authorisation.** Care must be taken to understand how the SNS being used works. Authorising 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.

289.1 **Whilst it is the responsibility of an individual to set privacy settings to protect unsolicited access to private information, and even though 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.** In some cases data may be deemed private communication still in transmission (instant messages for example). Where privacy settings are available but not applied the data may be considered open source and an authorisation is not usually required. Repeat viewing of “open source” sites may constitute directed surveillance on a case by case basis and this should be borne in mind.

289.2 **Providing there is no warrant authorising interception in accordance with section 48(4) of the 2000 Act, if it is necessary and proportionate for a public authority to breach covertly 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 a member of a public authority or by a person acting on its behalf (i.e. the activity is more than mere reading of the site’s content).

289.3 **It is not unlawful for a member of a public authority to set up a false identity but it is inadvisable for a member of a public authority to do so for a covert purpose without an authorisation for directed surveillance when private information is likely to be obtained.** The SRO should be satisfied that there is a process in place to ensure compliance with the legislation. Using photographs of other persons without their permission to support the false identity infringes other laws.

289.4 **A member of a public authority should not adopt the identity of a person known, or likely to be known, to the subject of interest or users of the site without authorisation, and without the consent of the person whose identity is used, and without considering the protection of that person.** The consent must be explicit (i.e. the person from whom consent is sought must agree preferably in writing) what is and is not to be done.
The council has developed a policy in relation to the use of social media for the gathering of evidence to assist in its enforcement activities is set out below:

- officers must not become ‘friends’ with individuals under any investigation on social networking sites
- officers must not use their own private accounts to view the social networking accounts of other individuals who may be under investigation
- officers viewing an individual’s profile on a social networking site should do so only once in order to obtain evidence to support or refute their investigation. Such viewing can take a backward look at the individual’s profile
- further viewing of open profiles on social networking sites to monitor an individual’s status, must only take place once RIPA authorisation has been granted and approved by a Magistrate.
- officers should be aware that it may not be possible to verify the accuracy of information on social networking sites and, if such information is to be used as evidence, steps must be taken to ensure its validity.

3. **DOES RIPA APPLY TO MY SITUATION?**

Ask yourself the following questions to see if RIPA applies to the surveillance that you want to carry out. Also check against the flowcharts in the appendices.

3.1 **Is the Surveillance Covert?**

RIPA only applies to covert surveillance.

For example, in the enforcement of private hire licensing, if a Licensing Officer flags down a private hire vehicle and identifies himself to the driver as a Licensing Officer immediately this would be ‘overt’ and RIPA will not apply.

However, if he rides as a passenger before making himself known as a Licensing Officer that would be covert.

3.2 **Is the surveillance for the purpose of a specific investigation or specific purpose?**

If the surveillance is directed at a known individual or group the provisions of RIPA will cover the investigation.

In respect of other situations, such as CCTV cameras that are readily visible to anyone walking around the area, their use is not governed by RIPA but is covered by the Data Protection Act, 1998. However, if the cameras are used as part of an operation to specifically observe a known individual or group or as part of a specific investigation it is very likely that RIPA will apply and an appropriate authorisation
will be required. This would also be covert as the individual would not know that cameras were specifically monitoring their activity.

3.2.1 Is the surveillance likely to obtain private information about a person?

If it is likely that observations will result in the obtaining of private information about any person, then RIPA may apply.

If in doubt, it is always safer to seek guidance and advice first.

3.3 Is the surveillance intrusive?

Directed surveillance turns into intrusive surveillance if it is carried out involving anything that occurs on residential premises or any private vehicle and involves the presence of someone on the premises or in the vehicle or is carried out by means of a (high quality) surveillance device. This could involve external CCTV recording images of the interior of a domestic premise, or a device which captures sound recordings.

If the device is not on the premises or in the vehicle, it is only intrusive surveillance if the device consistently produces information of the same quality as if it were.

Care needs to be taken when using equipment to monitor noise. If the equipment is sensitive enough (or the wall against which it is placed thin enough) to enable the picking up of conversation or other discernible noises then it may be intrusive.

REMEMBER - The Council is not permitted to carry out intrusive surveillance.

3.4 Is the surveillance an immediate response to an event or circumstances where it is not reasonably practicable to get authorisation?

It is not possible to give urgent authorisations orally. An application would have to made to a Magistrate for approval who may consider an authorisation out of hours in exceptional circumstances.

3.5 Is the surveillance for a purpose other than those specified in RIPA, such as monitoring of staff or telephone usage, e.g. To invoke the Council’s disciplinary process?

This type of surveillance is outside RIPA and does not need RIPA authorisation.

However this will come under the UK Data Protection Act, 1998 and the Lawful Business Practice Regulations, 2000 and, as such, can only normally be conducted if the subject is aware that such surveillance may be carried out by their acceptance
to Council policies in relation to management of staff, computers and telecommunications.

To provide safeguards no direct employee of the Council will undertake this monitoring, this will be undertaken by the Council’s Internal Audit Team who are appropriately authorised to do so.

If it is suspected that staff may be involved in activity which amounts to a criminal offence this must be reported immediately to your Line Manager or Internal Audit, who will ensure that any investigation and / or monitoring is carried out within the terms of the relevant legislation by liaison with the Council’s Information Governance Lead.

All Officers are also reminded of the Council’s Whistleblowing Policy.

3.6 Does the surveillance involve the use of a ‘source’?

If an individual is being used to establish a relationship with another person to obtain information then a RIPA authorisation is likely to be needed.

Where it is likely that a relationship will be established, the Council’s Information Governance Lead must be consulted prior to the relationship being progressed.

4 AUTHORISATION PROCEDURES

4.1 Any directed surveillance, or the use of a CHIS undertaken by or on behalf of the council must be carried out in accordance with RIPA and must not commence until authorisation has been granted and has been approved by a relevant judicial authority. If such activities are undertaken without authorisation the RIPA Monitoring Officer or Senior Responsible Officer must be advised immediately. Only those officers identified in Appendix 1 as Authorising Officers can authorise an application under RIPA. Once authorised, the application must be presented to a Magistrate for final approval.

4.2 Although the acquisition of communications data is covered separately to this policy, it must be noted that this can only be undertaken by a SPoC (although the same authorisation procedures will apply). If necessary the council would engage a third party to undertake this role.

4.3 Officers must discuss the need to undertake directed surveillance with their line manager before seeking an authorisation. All other reasonable and less intrusive options to gain the required information must be considered before an authorisation is applied for and the RIPA application must detail why these options have failed or have been considered not appropriate in the circumstances of the individual investigation.
4.4 All applications for authorisation must be made on the appropriate form. The forms can be found on the council’s intranet, insight together with a procedure for obtaining judicial approval. In the event of any query, officers making or authorising applications should consult the RIPA Monitoring Officer or the Senior Responsible Officer. The RIPA Monitoring Officer should be contacted prior to the completion of a RIPA application form so that a Unique Reference Number can be allocated.

4.5 Authorisations will not take effect until the relevant judicial authority has made an order approving the grant of the authorisation. The relevant judicial authority in England and Wales is a Magistrate. It is vital that any surveillance for which authorisation has been sought does not start until such time as it has been approved by a Magistrate.

4.6 It is necessary for the council to obtain judicial approval for all initial RIPA authorisations/applications and renewals. There is no requirement for the Magistrate to consider either cancellations or internal reviews.

4.7 The procedure for obtaining Magistrate approval can be found on the council’s intranet pages insight.

4.8 In the unlikely event that officers find it necessary to seek authorisation for the use of a CHIS, additional safeguards must be considered and advice must first be sought from the RIPA Monitoring Officer or Senior Responsible Officer.

4.9 In any case where it is likely that confidential information may be acquired by directed surveillance or by the use or conduct of a source, the Authorised Officer who may grant authorisation is the Head of Paid Service or, in his absence, the person acting as Head of Paid Service.

4.10 Confidential information consists of communications subject to legal privilege, communications between a Member of Parliament and another person on constituency matters, confidential personal information, or confidential journalistic material. So, for example, extra care should be taken where, through the use of surveillance, it is likely that knowledge will be acquired of communications between a minister of religion and an individual relating to the latter’s spiritual welfare, or between a Member of Parliament and a constituent relating to constituency matters, or wherever matters of medical or journalistic confidentiality or legal privilege may be involved.

4.11 When considering an application, Authorising Officers must:

(a) have regard to the contents of this document, the training provided and any other guidance or advice given by the RIPA Monitoring Officer or the Senior Responsible Officer;

(b) satisfy his/herself that the RIPA authorisation will be:
(i) in accordance with the law;
(ii) necessary in the circumstances of the particular case; and
(iii) proportionate to what it seeks to achieve.

(c) Assess whether or not the proposed surveillance is proportionate, considering the following elements:

- The custodial sentence applicable to the offence being investigated;
- Balancing the size and scope of the proposed activity against the gravity and extent of the perceived crime or offence;
- Explaining how and why the methods to be adopted will cause the least possible intrusion on the subject and others;
- Whether the activity is an appropriate use of the legislation and a reasonable way, having considered all practical alternatives, of obtaining the necessary result;
- Evidencing, as far as reasonably practicable, what other methods had been considered and why they were not implemented.

(d) take into account the risk of intrusion into the privacy of persons other than the specified subject of the surveillance (called ‘collateral intrusion’), and consider whether any measures should be taken to avoid or minimise collateral intrusion as far as possible (the degree of likely collateral intrusion will also be relevant to assessing whether the proposed surveillance is proportionate);

(e) consider any issues which may arise in relation to the health and safety of council employees and agents, and ensure that a risk assessment has been undertaken if appropriate.

4.12 When authorising the conduct or use of a CHIS, the Authorising Officer must also:

(a) be satisfied that the conduct and/or use of the CHIS is proportionate to the objective sought to be achieved;
(b) be satisfied that appropriate arrangements are in place for the management and oversight of the CHIS. These arrangements must address health and safety issues by the carrying out of a formal and recorded risk assessment;
(c) consider the likely degree of intrusion for all those potentially affected;
(d) consider any adverse impact on community confidence that may result from the use or conduct of the CHIS or the information obtained; and
(e) ensure that records contain the required particulars of the CHIS and that these are not available except on a ‘need to know’ basis.

4.13 Authorising Officers should consult the RIPA Monitoring Officer or the Senior Responsible Officer before authorising the use of conduct of a CHIS to ensure that all legal requirements are complied with.
4.14 If an application is granted, the Authorising Officer must set a date for its review, and ensure that it is reviewed on that. Records must be kept in relation to all RIPA applications and authorisations in accordance with paragraph 10 below, and to facilitate this, each investigation or operation should be given a unique reference number (URN) on the application form by the RIPA Monitoring Officer. This should be in the form:

Year / Business Unit / Number of Application.

Any subsequent forms (e.g. renewals or cancellations) relating to the same investigation or operation should be identified by means of the same URN.

5 URGENT AUTHORISATIONS

5.1 It is no longer possible for urgent authorisations to be given orally as Section 43(1)(a) of RIPA no longer applies to authorisations for directed surveillance or a CHIS. However, a Magistrate may consider an authorisation out of hours in exceptional circumstances.

6 DURATION OF AUTHORISATIONS

6.1 Authorisations will have effect until the date of expiry specified on the relevant form. They must be granted for the designated period of three months for directed surveillance, 12 months for the use or conduct of a CHIS and one month for the acquisition of communications data. No further operations should be carried out after the expiry of the relevant authorisation unless it has been renewed.

6.2 It will be the responsibility of the officer in charge of an investigation to ensure that any directed surveillance or use of a CHIS is only undertaken under an appropriate and valid authorisation, and therefore, he/she should be mindful of the date when authorisations and renewals will cease to have effect. The RIPA Monitoring Officer will perform an auditing role in this respect but the primary responsibility rests with the officer in charge of the investigation.

6.3 Authorisations should be reviewed at appropriate intervals in order to update the Authorising Officer on progress on the investigation and whether the authorisation is no longer required. Review periods should be set by the Authorising Officer, but should normally take place on a monthly basis unless the Authorising Officer considers that they should take place more or less frequently (if so, the reasons should be recorded). If the surveillance provides access to confidential information or involves collateral intrusion, there will be a particular need to review the authorisation frequently. The results of reviews should be recorded on the appropriate form.

6.4 Authorisations must be cancelled as soon as they are no longer necessary. Even if
an authorisation has reached its time limit and has ceased to have effect, it does not lapse and must still be formally cancelled. The responsibility for ensuring that authorisations are cancelled rests primarily with the officer in charge of the investigation, who should submit a request for cancellation on the appropriate form. However, if the Authorising Officer who authorised any directed surveillance or the use or conduct of a CHIS (or any Authorising Officer who has taken over their duties) is satisfied that it no longer meets the criteria upon which it was authorised, s/he must cancel it and record that fact in writing even in the absence of any request for cancellation.

6.5 If it is required, a renewal must be authorised prior to the expiry of the original authorisation. Applications for renewal should be made on the appropriate form shortly before the original authorisation period is due to expire. Officers must take account of factors which may delay the renewal process (e.g. intervening weekends or the availability of the relevant authorising officer and a Magistrate to consider the application). The Authorising Officer must consider the matter afresh, including taking into account the benefits of the surveillance to date and any collateral intrusion that has occurred. Renewals of an authorisation may be granted more than once, provided the criteria for granting that authorisation are still met. However, if the reason for requiring the authorisation has changed from the purpose for which it was originally granted, then it should be cancelled and new authorisation sought. The renewal will begin on the day when the authorisation would otherwise have expired.

6.6 In cancelling an authorization the Authorising Officer should:

- Record the date and times that surveillance took place and the order to cease activity was made
- Record the reason for the cancellation
- Ensure that any surveillance equipment is returned.
- Provide directions for the management of the product.
- Ensure that detail of the property interfered with, or person subjected to surveillance, since the last review is properly documented.
- Record the value of the surveillance or interference (whether the objective as set out in the authorisation were met).

7 MATERIAL OBTAINED DURING INVESTIGATIONS

7.1 Generally, all material (in whatever media) obtained or produced during the course of investigations subject to RIPA authorisations should be processed, stored and destroyed in accordance with the requirements of the Data Protection Act 1998, the Freedom of Information Act 2000, any other legal requirements, including those of confidentiality, and the council’s policies and procedures currently in force relating to document retention. The following paragraphs give guidance on some specific situations, but advice should be sought from the RIPA Monitoring Officer or the Senior Responsible Officer where appropriate.
7.2 Where material is obtained during the course of an investigation which might be relevant to that investigation, or another investigation, or to pending or future civil or criminal proceedings, then it should **not** be destroyed, but retained in accordance with legal disclosure requirements.

7.3 Where material is obtained, which is not related to a criminal or other investigation or to any person who is the subject of the investigation, and there is no reason to suspect that it will be relevant to any future civil or criminal proceedings, it should be destroyed immediately.

7.4 Material obtained in the course of an investigation may be used in connection with investigations other than the one that the relevant authorisation was issued for. However, the use or disclosure of such material outside the council, unless directed by any court order, should only be considered in exceptional circumstances, and in accordance with advice from the RIPA Monitoring Officer or the Senior Responsible Officer.

7.5 Where material obtained is of a confidential nature then the following additional precautions should be taken:

- Confidential material should not be retained or copied unless it is necessary for a specified purpose;
- Confidential material should only be disseminated in accordance with legal advice that it is necessary to do so for a specific purpose;
- Confidential material which is retained should be marked with a warning of its confidential nature. Safeguards should be put in place to ensure that such material does not come into the possession of any person where to do so might prejudice the outcome of any civil or criminal proceedings;
- Confidential material should be destroyed as soon possible after its use for the specified purpose.

If there is any doubt as to whether material is of a confidential nature, advice should be sought from the RIPA Monitoring Officer or the Senior Responsible Officer.

8 **ASSESSMENT AND REVIEW**

8.1 Following completion of any investigation / operation involving the use of RIPA, an independent assessment and review will be undertaken by the RIPA Monitoring Officer should be undertaken. This will consider the investigation, the methods, the information obtained and how it was used to take the case forward.

8.2 The outcome of the review will be retained by the RIPA Monitoring Officer and kept with the original paperwork. The review will be shared with the Senior Responsible Officer.

8.3 The SRO will review these periodically and will provide these records as part of any
inspection by the Office of Surveillance Commissioners.

9 **CCTV AND DIRECTED SURVEILLANCE**

9.1 The use of CCTV must be accompanied by clear signage in order for any monitoring to be overt. If it is intended to use CCTV for covert monitoring, for example by using either hidden cameras or without any signs warning that CCTV is in operation, then RIPA authorisation is likely to be required.

9.2 **Note 272 of the OSC’s 2016 Procedures & Guidance document:**

272. *It is recommended that a law enforcement agency should obtain a written protocol with a local authority if the latter’s CCTV system is to be used for directed surveillance. Any such protocol should be drawn up centrally in order to ensure a unified approach. The protocol should include a requirement that the local authority should see the authorisation (redacted if necessary to prevent the disclosure of sensitive information) and only allow its equipment to be used in accordance with it.*

10 **RECORDS MANAGEMENT**

10.1 Records shall be maintained for a period of six years from the cancellation of the authorisation. Following which they shall be securely destroyed in accordance with the council’s Records Retention Schedule.

10.2 The originals of all completed RIPA forms, including applications (whether granted or refused), authorisations, reviews, renewals and cancellations, must be forwarded by the Authorising Officer to the RIPA Monitoring Officer within *five working days* of the date of the relevant decision. All documents should be sent in sealed envelopes marked “Private and Confidential”.

10.3 Applicants and Authorising Officers may keep copies of completed RIPA forms, but care must be taken to ensure any copies are stored securely and disposed of in accordance with the council’s retention schedule. It is good practice for officers who will be carrying out surveillance to retain a copy of the authorisation as a reminder of exactly what has been authorised.

10.4 The following additional information should also be maintained by the Senior Responsible Officer or RIPA Monitoring Officer in relation to any CHIS:

- any risk assessment in relation to the source;
- the circumstances in which tasks were given to the source;
- the value of the source to the investigating authority;

10.5 The RIPA Monitoring Officer will hold responsibility for maintaining the Central
Register of Authorisations, but it the responsibility of Applicants and Authorizing Officers to notify the RIPA Monitoring Officer of any authorisations.

10.6 By law, an Authorising Officer must not grant authority for the use of a CHIS unless s/he believes that there are arrangements in place for ensuring that there is at all times a person with the responsibility for maintaining a record of the use made of the CHIS. Certain particulars must be included in the records relating to each CHIS, and the records must be kept confidential. Further advice should be sought from the RIPA Monitoring Officer or Senior Responsible Officer on this point if authority is proposed to be granted for the use of a CHIS.

10.7 A ‘Surveillance Log Book’ should be completed by the investigating officer(s) to record all operational details of authorised covert surveillance or the use of a CHIS. Once completed, the Log Book shall be passed to the Head of the relevant Service Area.

10.8 All RIPA records, whether in original form or copies shall be kept in secure locked storage when not in use.

11 TRAINING

11.1 Appropriate corporate training will be arranged by the RIPA Monitoring Officer for all officers likely to make applications or authorise them.

11.2 The RIPA Monitoring Officer will ensure suitable training is in place for all new members of staff who undertake an enforcement role. Managers of enforcement teams must ensure new staff undertake RIPA training within six months of their starting date.

11.3 Authorising Officers must receive appropriate training. This may be by way of a briefing or an e-learning module at a frequency as the RIPA Monitoring Officer deems appropriate.

11.4 All other identified staff will re, either by way of a briefing or an e-learning module. It is the responsibility of managers of enforcement teams in particular, to ensure relevant staff are identified and receive such training.

11.5 Officers may in any event supplement this corporate training by attending appropriate external training courses and seminars. The cost of such external training should be met from the budget of the individual Service Area.

11.6 No officer will be permitted to undertake the role of Applicant or Authorising Officer unless she/he has undergone suitable training approved by the RIPA Monitoring Officer.
Appendix One: RIPA Management Structure

Audit Committee – Policy Review and Elected Member Oversight

Steve Parrock
Chief Executive

Caroline Taylor
Director Adult Services
Senior Responsible

Jo Beer
Corporate Support Manager & Data Protection Officer
Monitoring / Co-ordinating Officer

Fran Hughes
Assistant Director
Community & Customer Services
Authorising Officer

Kevin Mowat
Executive Head
Business Services
Authorising Officer

Anne-Marie Bond
Assistant Director Corporate & Business Services (Monitoring Officer)
Designated Officer Communications Data

Steve Cox
Environmental Health Manager (resp. for CCTV)

National Anti-Fraud Network (NAFN) SPoC
Appendix Two: Flowchart 1 - Are you conducting Directed Surveillance?

Are you doing "surveillance"?
S.48(2)-(4)

NO

Are you doing "surveillance"?
S.48(2)-(4)

YES

Is the surveillance "covert"?
S.26(9)(a)

NO

Is the surveillance "covert"?
S.26(9)(a)

YES

Is it for a specific investigation or a specific operation?
S.26(2)(a)

NO

Is it for a specific investigation or a specific operation?
S.26(2)(a)

YES

Is the surveillance undertaken in such a manner as is likely to result in the obtaining of private information about a person?
S.26(10)

NO

Is the surveillance undertaken in such a manner as is likely to result in the obtaining of private information about a person?
S.26(10)

YES

Is the surveillance an immediate response to events or circumstances?
S.26(2)(c)

YES

DIRECTED SURVEILLANCE
Consider Authorisation
Also consider if involves Intrusive Surveillance as well – check flowchart 2

SEEK MAGISTRATES’ APPROVAL

NOT DIRECTED SURVEILLANCE

But still need to consider:
- Article 8 of the ECHR (privacy)
- the completion of a non RIPA surveillance authorisation form

NO RIPA ISSUE

NO

NO

NO
Appendix Three: Flowchart 2 - Are you doing Intrusive Surveillance?

- Are you doing "surveillance"? S.48(2)-(4)
  - NO
    - NO RIPA ISSUE
  - YES
    - Is the surveillance "covert"? S.26(9)(a)
      - NO
        - NOT DIRECTED OR INTRUSIVE SURVEILLANCE (But still need to consider Article 8 ECHR - right to privacy)
      - YES
        - Is the surveillance being carried out in relation to anything taking place on residential premises or in a private vehicle? S.26(3)(a) & S.81
          - NO
            - NOT INTRUSIVE SURVEILLANCE BUT COULD BE DIRECTED (See flowchart 1)
          - YES
            - Is it being done by using a surveillance device? S.26(3)(b)
              - NO
                - YES
                  - Is the device on or inside the premises or vehicle? S.26(3)(b)
                    - NO
                      - NO
                        - YES
                          - Does the device give same level of detail as from a device on the premises? S.26(5)(b)
                            - NO
                              - YES
                                - N.B. Cannot be authorised by local authorities

- INTRUSIVE SURVEILLANCE

N.B. Cannot be authorised by local authorities
Appendix Four: Flowchart 3 – Are you deploying a CHIS?

1. Are you using a person to obtain or provide access to information for you?
   - NO: NO RIPA ISSUE
   - YES:
     2. Will he/she be establishing or maintaining a personal or other relationship with another person?
        - NO:
        - YES:
            3. Will he/she be doing this for the covert purpose of covertly using such a relationship to obtain information or to provide access to any information to another person?
               - NO:
               - YES:
                   4. Will he/she be doing this for the covert purpose of covertly disclosing information obtained by the use of such a relationship, or as a consequence of the existence of such a relationship?
                      - NO:
                      - YES: SEEK MAGISTRATES’ APPROVAL

CHIS SITUATION
Consider Authorisation
Appendix Five: Flowchart 4 – Authorising Directed Surveillance

**Q.1 – Is the surveillance necessary?**

**Q.2 – Is the surveillance proportionate?**

See para 3.6 of Covert Surveillance Code – Consider:
- Size and scope of operation
- Methods to be adopted
- Alternative means available
- Appropriate use of legislation
- Impact on suspect

*Does it involve preventing or detecting a serious offence*?  
*One carrying a term of imprisonment of six months or more*

**Q.3 – Have you considered what you can do (if anything) to minimise/avoid collateral intrusion?**

See para 3.8 of Covert Surveillance Code - Consider e.g.:
- Size and scope of operation
- Means/equipment used
- Timing of surveillance
- Duration of surveillance

**Does it involve preventing or detecting a serious offence?**

**Is it to prevent or detect an offence-involving sale of tobacco or alcohol to underage children?**

**CANNOT BE AUTHORISED AS DIRECTED SURVEILLANCE**

**AUTHORISE AS DIRECTED SURVEILLANCE**

**SEEK MAGISTRATES’ APPROVAL**
Appendix Six: Flowchart 5 – Authorising a CHIS

Q.1 - Is the deployment of the CHIS necessary in the interests of preventing or detecting crime or preventing disorder?

Q.2 - Is the deployment of the CHIS proportionate?

See para 3.5 of the CHIS Code. Consider:

- Size and scope of operation
- Methods to be adopted
- Alternative means available
- Appropriate use of legislation

Q.3 - Have you considered what you can do (if anything) to minimise/avoid collateral intrusion?

See para 3.8 of the CHIS Code. Consider e.g.:

- Size and scope of operation
- Means/equipment used
- Timing of surveillance

Q.4 - Have you complied with the Special Duties?

See S.29(5) of RIPA and Chapter 6 and 7 of the CHIS Code – Consider:

- Security and welfare of CHIS
- CHIS Handler
- CHIS Controller
- Source records

YES

CANNOT BE AUTHORISED AS A CHIS

NO

YES

YE

SEEK MAGISTRATES’ APPROVAL

NO

YES

AUTHORISE AS A CHIS
Appendix Seven: Flowchart 6 - The Magistrates’ Approval Process

1. Complete authorisation form and seek approval of Authorising Officer

2. Complete judicial approval application form

3. Contact local Magistrates’ Court to arrange a hearing

4. Attend court with:
   - Counter-signed RIPA authorisation form plus a copy
   - Judicial approval application form plus copy
   - Any other relevant reference or supporting material

5. **MAGISTRATES’ DECISION OPTIONS**

   - **REFUSE TO APPROVE** and quash the authorisation due to fundamental flaw
     (2 days to make further representations)

   - **REFUSE TO APPROVE** authorisation due to a technical issue
     (Make correction and re-submit to court)

   - **APPROVE THE AUTHORISATION**
     Council can go ahead with the surveillance