



## **CORPORATE POLICY & PROCEDURES DOCUMENT**

**ON**

## **THE REGULATION OF INVESTIGATORY POWERS ACT 2000**

**(RIPA)**

**Mirza Ahmad MBA LLM Barrister  
Corporate Director of Governance (& Monitoring Officer)  
Ingleby House  
11-14 Cannon Street  
Birmingham B2 5EN**

Tel: 0121 303 9991

Fax: 0121 303 1312

E-mail: [mirza\\_ahmad@birmingham.gov.uk](mailto:mirza_ahmad@birmingham.gov.uk)

Re-issued date: 20 September 2004

Amended in June 2006 and finalised September 2006

Updated March 2007, November 2007, June 2008, October 2008, April 2010, March 2011, April 2011

# CONTENTS PAGE

	<u>Page No</u>	
<b>A</b>	<b>Introduction and Key Messages .....</b>	<b>3</b>
<b>B</b>	<b>City Council Policy Statement .....</b>	<b>4</b>
<b>C</b>	<b>Effective Date of Operation: 1 April 2003 and Authorising Officer Responsibilities .....</b>	<b>5</b>
<b>D</b>	<b>General Information on RIPA .....</b>	<b>6</b>
<b>E</b>	<b>What RIPA Does and Does Not Do .....</b>	<b>7</b>
<b>F</b>	<b>Types of Surveillance .....</b>	<b>8</b>
<b>G</b>	<b>Conduct and Use of a Covert Human Intelligence Source (CHIS) .....</b>	<b>11</b>
<b>H</b>	<b>Acquisition of Communications Data .....</b>	<b>13</b>
<b>I</b>	<b>Authorisation Procedures .....</b>	<b>14</b>
<b>J</b>	<b>Working with / through Other Agencies .....</b>	<b>18</b>
<b>K</b>	<b>Record Management .....</b>	<b>19</b>
<b>L</b>	<b>Concluding Remarks of the Corporate Director of Governance ...</b>	<b>20</b>
	<b>Appendix 1 - List of Authorising Officer Posts</b>	
	<b>Appendix 2 – RIPA Flow Charts for Directed Surveillance</b>	
	<b>Appendix 3 – RIPA A Forms: Directed Surveillance</b>	
	<b>Appendix 4 – RIPA B Forms: Covert Human Intelligence Source (CHIS)</b>	
	<b>Additional Notes and Flowchart on CHIS</b>	
	<b>Appendix 5 – Acquisition of Communications Data Forms, Guidance Notes and Flowchart</b>	
	<b>Appendix 6 – Home Office Code of Practice on Surveillance</b>	
	<b>Appendix 7 – Home Office Codes of Practice on CHIS</b>	
	<b>Appendix 8 – Employee Surveillance Forms</b>	

**NB:** The Regulation of Investigatory Powers Act 2000 ('RIPA') refers to 'Designated Officers'. For ease of understanding and application within Birmingham City Council, this Corporate Policy & Procedures Document refers to 'Authorising Officers'. Furthermore, such Officers can only act under RIPA if they have been duly certified by the Council's Corporate Director of Governance. For the avoidance of doubt, therefore, all references to duly certified Authorising Officers refer to 'Designated Officers' under RIPA.

## **Acknowledgements:**

- *The City Council is most grateful to Lord Colville of Culross, Assistant Commissioner of the Office of Surveillance Commissioners, for:*
    - a) *conducting an audit of the City Council's policy and procedures in January 2003; and*
    - b) *his most instructive and helpful contributions to the development of this Corporate Policy & Procedures Document.*
  
  - *Extract from a letter dated 13 May 2005 from The Rt Hon, Sir Andrew Leggatt on the visit/review by his Assistant Surveillance Commissioner, His Honour Jeremy Fordham on 15 April 2005:*  
*"Conclusions – Birmingham, following Lord Colville's recommendations, has established an admirable implementation of the RIPA requirements. A sound framework is in place and is being widely and responsibly used".*
- If any local authority adopts or adapts this Document for its purposes, please acknowledge Birmingham City Council's work in this area.**

## A. Introduction and Key Messages

1. This Corporate Policy & Procedures Document is based upon the requirements of The Regulation of Investigatory Powers Act 2000 ('RIPA') and Home Office's Code of Practices on Covert Surveillance and Covert Human Intelligence Sources. Covert surveillance should be used only rarely and in exceptional circumstances. Copies of the Home Office's Codes of Practice are attached and also available on their website. The website codes should be consulted, from time to time, to ensure this Document remains up to date.
2. The City Council acknowledges the most constructive help and support it has received from The Office of the Surveillance Commissioners and, in particular, Lord Colville of Culross, an Assistant Commissioner of the Office of Surveillance Commissioners, who audited, in January 2003, the City Council's implementation of RIPA requirements and who reviewed and commented upon a draft of this Corporate Policy and Procedures Document ('this Document'). The City Council also takes responsibility for ensuring the RIPA procedures are continuously improved.
3. The authoritative position on RIPA is, of course, the Act itself and any Officer who is unsure about any aspect of this Document should, if unsure, **contact, at the earliest possible opportunity, the Council's Corporate Director of Governance, for advice and assistance.** Appropriate training and development (including refresher training) will be organised by the Corporate Director of Governance for relevant Authorising Officers and other senior managers. Even though the Act refers to "designated officers", such officers are "Authorising Officers" in the Birmingham context and throughout this Document. Copies of this Document and related Forms will be placed on Lotus Notes.
4. The Corporate Director of Governance will maintain and check the Corporate Register of all RIPA Authorisations, Reviews, Renewals, Cancellations and rejections. From April 2007, for applications for covert surveillance, an electronic database has been developed and access has been provided to designated applicants and appropriate Authorising Officers to manage all aspects of the RIPA process. Applications for Communications Data and CHIS, will, for the time being remain paper based.
5. RIPA and this Document are important for the effective and efficient operation of the City Council's actions with regard to covert surveillance and Covert Human Intelligence Sources. This Document will, therefore, be kept under 6-monthly review by the Corporate Director of Governance. **Authorising Officers must bring any suggestions for continuous improvement of this Document to the attention of the Corporate Director of Governance at the earliest possible opportunity.** If any of the Home Office Codes of Practice change, this Document will be amended in light of these changes.
6. In terms of monitoring e-mails and internet usage, it is important to recognise the important interplay and overlaps with the City Council's e-mail and internet policies and guidance, the Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000, the Data Protection Act 1998 and its Codes of Practice. Under normal circumstances, the Council's e-mail and Internet policies should be used, as any surveillance is likely to be more relevant under the contract of employment terms as opposed to RIPA.
7. **At no time should the Council undertake any surveillance that interferes with any private property. Placing tracking devices on a subject's vehicle or person are not authorised for local authorities and must not be used. Again, if anyone is under any doubt on RIPA, this Document or the related legislative provisions, please consult the Corporate Director of Governance, at the earliest possible opportunity.**

## **B. City Council Policy Statement**

1. The City Council takes seriously its statutory responsibilities and will, at all times, act in accordance with the law and take necessary and proportionate action in these types of matters. In that regard, the Corporate Director of Governance, is duly authorised by the Council to keep this Document up to date and to amend, delete, add or substitute relevant provisions, as necessary. For administration and operational effectiveness, the Corporate Director of Governance is also authorised to add or substitute Officers authorised for the purpose of RIPA.
2. The City Council's Executive Committee on 25 September 2000, resolved as follows:
  - (a) that all covert surveillance exercises conducted by the Council should comply with the requirements of RIPA;
  - (b) that only the Chief Officer responsible for the Directorate proposing to undertake covert surveillance be permitted to authorise a covert surveillance exercise; and
  - (c) that this Report be referred to all those Advisory Teams which may carry out covert surveillance.
3. Since then there have been two internal audits and a further report to the Executive Committee on 28 September 2001.
4. This Document was circulated to the OSC, relevant Chief Officers and other Senior Managers, in draft format, on 11 February 2003. On the 24 February 2003, the City Council's Cabinet resolved as follows:-
  - (i) noted the constructive and helpful outcome to the OSC Audit;
  - (ii) approved the Draft 'Corporate & Policy Procedure Document on RIPA'; and
  - (iii) authorised the Corporate Director of Governance to do all that was necessary to conclude the matter with the OSC subject to any further inspection, establish the necessary corporate procedures and ensure all departments implement and comply with the Corporate Policy & Procedures Document with effect from 1 April 2003.
5. During 2006, two inspections by the Office of the Surveillance Commissioner were conducted into the City Council's use of RIPA procedures. Criticisms from those inspections have resulted in further training for authorising officers and applicants as well as additional guidance from the Corporate Director of Governance.
6. A further inspection by the Office of the Surveillance Commissioner took place in November 2007 and the report of the OSC commended the Council in the improvements that it had made to strengthen its compliance with RIPA.
7. In March 2010, Lord Colville of Culross, inspected the Council's use of RIPA and also provided an update on the changes resulting from the revised RIPA Codes of Practice for Directed Surveillance and Covert Human Intelligence Sources, which came into force in April 2010. The changes recommended from both the inspection and the codes of practice have been incorporated into this document.

**C. Effective Date of Operation : 1 April 2003  
And Authorising Officer Responsibilities**

1. The Corporate Policy, Procedures and the Forms provided in this Document became operative with effect from 1 April 2003. It is essential, therefore, that Chief Officers and Authorising Officers in their Departments, take personal responsibility for the effective and efficient operation of this Document in their Departments. The forms were revised, in June 2006, following a critical Office of Surveillance Commissioners Report and the Home Office forms have been incorporated in this Document. These forms have, subsequently, been used as the basis for the electronic database for applications for directed surveillance.
2. The Corporate Director of Governance has and will ensure that a sufficient number of Authorising Officers from each Department are, after suitable training on RIPA and this Document, duly certified to take action under this Document.
3. **It will be the responsibility of Authorising Officers (who have been duly certified) to ensure their relevant members of staff are suitably trained as 'Applicants' so as to avoid common mistakes appearing on Forms for RIPA authorisations.**
4. **Authorising Officers will also ensure that staff who report to them follow this Corporate Policy & Procedures Document and do not undertake or carry out any form of surveillance without first obtaining the relevant authorisations in compliance with this Document.**
5. Authorising Officers must also pay particular attention to Health and Safety issues that may be raised by any proposed surveillance activity. Under no circumstances, should an Authorising Officer approve any RIPA form unless, and until s/he is satisfied the health and safety of Council employees/agents are suitably addressed and/or risks minimised, so far as is possible, and proportionate to/with the surveillance being proposed. If an Authorising Officer is in any doubt, s/he should obtain prior guidance on the same from his/her Chief Officer, the City Council's Health & Safety Officer and/or the Corporate Director of Governance.
6. Authorising Officers must acquaint themselves with the relevant Codes of Practice issued by the Home Office regarding RIPA. Any failure to comply exposes the City Council to unnecessary legal risks and criticism from the Office of Surveillance Commissioners. Cancellations must be promptly dealt with.
7. Coming across **confidential information** during a surveillance must be given prior thought before any applications are authorised, as failure to do so may invalidate the admissibility of any evidence obtained. Furthermore, thought must be given before any forms are signed to the retention and disposal of any material obtained under a RIPA Authorisation. Where there is any possibility of confidential information being obtained through covert surveillance, the application must be authorised by the Chief Executive, or in his absence, the Corporate Director of Governance.
8. The Authorising Officer must ensure proper regard is had to **necessity and proportionality** before any applications are authorised. 'Stock phrases' or cut and paste narrative must be avoided at all times as the use of the same may suggest that insufficient detail had been given to the particular circumstances of any person likely to be the subject of the claim. Any **equipment** to be used in any approved surveillance must also be properly controlled, recorded and maintained for audit purposes.

## D. General Information on RIPA

1. The Human Rights Act 1998 (which brought much of the European Convention on Human Rights and Fundamental Freedoms 1950 into UK domestic law) requires the City Council, and organisations working on its behalf, pursuant to Article 8 of the European Convention, to respect the private and family life of citizens, his home and his correspondence.
2. The European Convention did not, however, make this an absolute right, but a qualified right. Accordingly, in certain circumstances, the City Council may interfere in the citizen's right mentioned above, if such interference is:-
  - (a) **in accordance with the law;**
  - (a) **necessary** (as defined in this Document); **and**
  - (b) **proportionate** (as defined in this Document).
3. The Regulation of Investigatory Powers Act 2000 ('RIPA') provides a statutory mechanism (i.e. 'in accordance with the law') for authorising **covert surveillance** and the use of a '**covert human intelligence source**' ('CHIS') – e.g. undercover agents. It now also permits Public Authorities to compel telecommunications and postal companies to obtain and release communications data to themselves, in certain circumstances. It seeks to ensure that any interference with an individual's right under Article 8 of the European Convention is necessary and proportionate. In doing so, the RIPA seeks to ensure both the public interest and the human rights of individuals are suitably balanced.
4. Directly employed Council staff and external agencies working for the City Council are covered by the Act for the time they are working for the City Council. All external agencies must, therefore, comply with RIPA and the work carried out by agencies on the Council's behalf must be properly authorised by one of the Council's Authorising Officers. Authorising Officers are those whose posts appear in **Appendix 1** to this Document and, duly certified, added to or substituted to by the Corporate Director of Governance.
5. If the correct procedures are not followed, evidence may be disallowed by the courts, a complaint of maladministration could be made to the Ombudsman, and/or the Council could be ordered to pay compensation. Such action would not, of course, promote the good reputation of the City Council and will, undoubtedly, be the subject of adverse press and media interest. It is essential, therefore, that all involved with RIPA comply with this Document and any further guidance that may be issued, from time to time, by the Corporate Director of Governance.
6. Flowcharts of the procedures to be followed appear at **Appendix 2** for Directed Surveillance and for CHIS.

## **E. What RIPA Does and Does Not Do**

### **1. RIPA does:**

- require prior authorisation of directed surveillance.
- prohibit the Council from carrying out intrusive surveillance.
- compels disclosure of communications data from telecom and postal service providers.
- require authorisation of the conduct and use of a CHIS.
- require safeguards for the conduct and use of a CHIS.
- permit the Council to obtain Communications records from Communications service providers.

### **2. RIPA does not:**

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

### **3. If the Authorising Officer or any Applicant is in any doubt, s/he should ask the Corporate Director of Governance BEFORE any directed surveillance and/or CHIS is authorised, renewed, cancelled or rejected.**

## F. Types of Surveillance

### 1. 'Surveillance' includes

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

Surveillance can be overt or covert.

### 2. Overt Surveillance

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

3. Similarly, surveillance will be overt if the subject has been told it will happen (e.g. where a noisemaker is warned (preferably in writing) that noise will be recorded if the noise continues, or where an entertainment licence is issued subject to conditions, and the licensee is told that officers may visit without notice or identifying themselves to the owner/proprietor to check that the conditions are being met.

### 4. Covert Surveillance

Covert Surveillance is carried out in a manner calculated to ensure that the person subject to the surveillance is unaware of it taking place. (Section 26(9)(a) of RIPA). It cannot, however, be “necessary” if there is reasonably available an overt means of finding out the information desired.

5. RIPA regulates two types of covert surveillance, (Directed Surveillance and Intrusive Surveillance) and the use of Covert Human Intelligence Sources (CHIS).

### 6. Directed Surveillance

Directed Surveillance is surveillance which:-

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

7. Private information in relation to a person includes any information relating to his private and family life, his home and his correspondence. The fact that covert surveillance occurs in a public place or on business premises does not mean that it cannot result in the obtaining of private information about a person. Prolonged surveillance targeted on a single person will undoubtedly result in the obtaining of private information about him/her and others that s/he comes into contact, or associates, with.
8. Similarly, although overt town centre CCTV cameras do not normally require authorisation, if the camera(s) are to be directed for a specific purpose to observe particular individual(s), authorisation will be required. The way a person runs his/her business may also reveal information about his or her private life and the private lives of others.
9. **For the avoidance of doubt, only those Officers designated and certified to be 'Authorising Officers' for the purpose of RIPA can authorise 'Directed Surveillance' IF, AND ONLY IF, the RIPA authorisation procedures detailed in this Document are followed. If an Authorising Officer has not been 'certified' for the purposes of RIPA, s/he can **NOT** carry out or approve/reject any action set out in this Corporate Policy & Procedures Document. For further information about Authorising Officers, please see paragraph 12. Access to the electronic database (for Directed Surveillance) will only be provided to those officers who have been duly 'certified'.**

10. **Intrusive Surveillance**

This is when it:-

- 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 is carried out by a surveillance device in the premises/vehicle. Surveillance equipment mounted outside the premises will not be intrusive, unless the device consistently provides information of the same quality and detail as might be expected if they were in the premises/vehicle.

11. **This form of surveillance cannot be carried out or approved by the Council. Only the police and other law enforcement agencies are permitted to use such powers. Likewise, the Council has no statutory powers to interfere with private property.**

12. **Tracking Devices and Vehicle Tracking Devices**

Tracking devices to be used in or on skips can be authorised by Authorising Officers, provided that the tracking device is disguised as refuse and is not physically attached/affixed to the skip. They do not need prior approval from the Corporate Director of Governance.

Due to uncertainty as to the legal position as to the use of Vehicle Tracking devices, any proposals for the use of Vehicle Tracking Devices need to be discussed with the Corporate Director of Governance so that a decision can be made on the matter in light of the circumstances in which the vehicle tracking device might be used. As any interference with property will require RIPA authorisation from the Police, a Local Authority is not entitled to interfere with property for the purposes of surveillance. The Corporate Director of Governance will only authorising vehicle tracking devices in cases where there is no interference with property.

In the event of there being a requirement that vehicle tracking device be used, and that to install/affix such a device, interference with property not owned by Birmingham City Council

will occur it is recommend that the RIPA authorisation from the Police be used in those circumstances.

### 13 **Employee Surveillance using covert surveillance**

Following a recent decision of the Surveillance Tribunal, it has been established that RIPA authorisation is not required where the surveillance is undertaken as part of an investigation in relation to an employee's misconduct or breach of the terms and conditions of the employee's contract of employment, i.e. any investigation undertaken other than into an alleged criminal offence.

However, such surveillance may still potentially be viewed as infringing the employee's right to privacy as established under Article 8 of the Human Rights Act.

Where such surveillance, pertaining to a non-criminal investigation into the conduct of an employee, is required, officers are required to complete the appropriate form, as set out in Appendix 8 and then forward the form to their authorising officer for approval.

For purposes of consistency, authorisations will last for 3 months and appropriate action must be taken to review, renew and cancel authorisations.

The authorising officer will apply the same criteria as if the request was for RIPA authorisation.

Once authorised, a signed copy of the authorised form and subsequent review, renewal and cancellation forms must be kept secure with the investigation file. **There is no requirement to log the authorisation on the Corporate Database.**

### 14. **"Proportionality"**

The term contains three concepts:-

- the means should not be excessive by relation to the gravity of the mischief being investigated;
- the least intrusive means of surveillance should be chosen; and
- collateral intrusion involves invasion of third parties' privacy and should, so far as is possible, be minimised.

In other words, this involves balancing the intrusiveness of the activity on the target subject and others who might be affected by it against the need for the activity in operational terms. The activity will not be proportionate if it is excessive in the circumstances – each case will be judged and be unique on its merits – or if the information which is sought could be reasonably be obtained by other less intrusive means. All such activity must be carefully managed to meet the objective in question and must not be arbitrary or unfair. Extra care should also be taken over any publication of the product of the surveillance.

It is important that when setting out the proportionality of the surveillance, that the applications include clear statements of the other reasonably possible methods of obtaining the desired information and the reasons why they have been rejected. This approach will apply, equally, to arguments for the necessity of the surveillance.

In the event of a challenge to the surveillance, the courts will assess whether what was authorised was both necessary and proportionate for the purpose of the investigation. The Act requires that the Authorising officer should have believed this to be the case before granting an authorisation. Thus, it would primarily be to the authorising officer's comments that attention would be paid. It is important, therefore, that Authorising officer's express

their own view, rather than referring back to and relying on the explanations given by the applicant.

15. **Examples of different types of Surveillance**

<b>Type of Surveillance</b>	<b>Examples</b>
<u>Overt</u>	<ul style="list-style-type: none"> <li>- Police Officer or Parks Warden on patrol</li> <li>- Signposted Town Centre CCTV cameras (in normal use)</li> <li>- Recording noise coming from outside the premises after the occupier has been warned that this will occur if the noise persists.</li> <li>- Most test purchases (where the officer behaves no differently from a normal member of the public).</li> </ul>
<u>Covert</u> but not requiring prior authorisation	<ul style="list-style-type: none"> <li>- CCTV cameras providing general traffic, crime or public safety information.</li> </ul>
<u>Directed</u> must be RIPA authorised.	<ul style="list-style-type: none"> <li>- Officers follow an individual or individuals over a period, to establish whether s/he is working when claiming benefit or off long term sick from employment.</li> <li>- Test purchases where the officer has a hidden camera or other recording device to record information which might include information about the private life of a shop-owner, e.g. where s/he is suspected of running his business in an unlawful manner.</li> </ul>
<u>Intrusive or interfering with private property</u> – <b>City Council cannot do this!</b>	<ul style="list-style-type: none"> <li>- Planting a listening or other electronic device (bug) or camera in a person's home or in / on their private vehicle / person.</li> </ul>

**Further Information**

16. Further guidance on surveillance can be found in the Home Office Code of Practice on surveillance, at Appendix 6 and at:

[www.homeoffice.gov.uk/crimpol/crimreduc/regulatobn/codesofpractice.html](http://www.homeoffice.gov.uk/crimpol/crimreduc/regulatobn/codesofpractice.html)

17. **Confidential Information**

Special safeguards apply with regard to confidential information relating to legal privilege, personal information and journalistic material. The Authorising Officer and the person carrying out the surveillance must understand that such information is confidential and can not be obtained. Further guidance is available in the Home Office Codes of Practice.

18. **Collateral Intrusion**

Before authorising surveillance the authorising officer should also take into account the risk of intrusion into the privacy of persons other than those who are directly the subjects of the investigation or operation (collateral intrusion). Measures should be taken, wherever practicable, to avoid or minimise unnecessary intrusion into the lives of those not directly connected with the investigation or operation.

Those carrying out the surveillance should inform the authorising officer if the investigation or operation unexpectedly interferes with the privacy of individuals who are not covered by the authorisation. When the original authorisation may not be sufficient, consideration should be given to whether the authorisation needs to be amended and reauthorised or a new authorisation is required.

Further guidance is available in the Home Office Codes of Practice.

19, **Retention and destruction of product of surveillance**

Where the product of surveillance could be relevant to pending or future criminal or civil proceedings, it should be retained in accordance with established disclosure requirements for a suitable period and subject to review.

There is nothing in RIPA which prevents material obtained from properly authorised surveillance from being used in other investigations. Authorising Officers must ensure, therefore, that arrangements are in place for the handling, storage and destruction of material obtained through the use of covert surveillance. Authorising Officers must also ensure compliance with the appropriate data protection requirements and any relevant codes of practice produced by individual authorities relating to the handling and storage of material.

## **G. Conduct and Use of a Covert Human Intelligence Source (CHIS)**

### **Who is a CHIS?**

1. Someone who establishes or maintains a personal or other relationship for the covert purpose of helping the covert use of the relationship to obtain information.
2. RIPA does not apply in circumstances where members of the public volunteer information to the City Council as part of their normal civic duties, or to contact numbers set up to receive information.

### **What must be authorised?**

3. The Conduct or Use of a CHIS require prior authorisation.
  - **Conduct** of a CHIS = Establishing or maintaining a personal or other relationship with a person for the covert purpose of (or is incidental to) obtaining and passing on information.
  - **Use** of a CHIS = Actions inducing, asking or assisting a person to act as a CHIS and the decision to use a CHIS in the first place.
4. **The Council can use CHIS's IF, AND ONLY IF THE RIPA procedures, as detailed in this Document, are followed. Authorisation for CHIS's can only be granted if it is for the purposes of "preventing or detecting crime or of preventing disorder".**
5. Record keeping:  
**Particulars to be contained in records**  
The following matters are specified for the purposes of paragraph (d) of section 29(5) of the 2000 Act (as being matters particulars of which must be included in the records relating to each source):
  - (a) the identity of the source;
  - (b) the identity, where known, used by the source;
  - (c) any relevant investigating authority other than the authority maintaining the records;
  - (d) the means by which the source is referred to within each relevant investigating authority;
  - (e) any other significant information connected with the security and welfare of the source;
  - (f) any confirmation made by a person granting or renewing an authorisation for the conduct or use of a source that the information in paragraph (d) 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;
  - (g) the date when, and the circumstances in which, the source was recruited;
  - (h) the identities of the persons who, in relation to the source, are discharging or have discharged the functions mentioned in section 29(5)(a) to (c) of the 2000 Act or in any order made by the Secretary of State under section 29(2)(c);

- (i) the periods during which those persons have discharged those responsibilities;
- (j) the tasks given to the source and the demands made of him in relation to his activities as a source;
- (k) all contacts or communications between the source and a person acting on behalf of any relevant investigating authority;
- (l) the information obtained by each relevant investigating authority by the conduct or use of the source;
- (m) any dissemination by that authority of information obtained in that way; and
- (n) in the case of a source who is not an undercover operative, every payment, benefit or reward and every offer of a payment, benefit or reward that is made or provided by or on behalf of any relevant investigating authority in respect of the source's activities for the benefit of that or any other relevant investigating authority.

### **Juvenile Sources**

- 5. Special safeguards apply to the use or conduct of juvenile sources (i.e. under 18 year olds). On no occasion can a child under 16 years of age be authorised to give information against his or her parents. Only the Chief Executive and/or the Corporate Director of Governance are duly authorised by the City Council to use Juvenile Sources, as there are other onerous requirements for such matters.

### **Vulnerable Individuals**

- 6. A Vulnerable Individual is a person who is or may be in need of community care services by reason of mental or other disability, age or illness and who is or may be unable to take care of himself or herself, or unable to protect himself or herself against significant harm or exploitation.
- 7. A Vulnerable Individual will only be authorised to act as a source in the most exceptional of circumstances. Only the Chief Executive and/or the Corporate Director of Governance, are duly authorised by the City Council to use Vulnerable Individuals, as there are other onerous requirements for such matters.

### **Test Purchases**

- 8. Carrying out test purchases will not (as highlighted above) require the purchaser to establish a relationship with the supplier with the covert purpose of obtaining information and, therefore, the purchaser will not normally be a CHIS. For example, authorisation would not normally be required for test purchases carried out in the ordinary course of business (e.g. walking into a shop and purchasing a product over the counter).
- 9. By contrast, developing a relationship with a person in the shop, to obtain information about the seller's suppliers of an illegal product (e.g. illegally imported products will require authorisation as a CHIS. Similarly, using mobile hidden recording devices or CCTV cameras to record what is going on in the shop will require authorisation as directed surveillance. A combined authorisation can be given for a CHIS and also directed surveillance.

**Anti-social behaviour activities (e.g. noise, violence, race etc)**

10. Persons who complain about anti-social behaviour, and are asked to keep a diary, will not normally be a CHIS, as they are not required to establish or maintain a relationship for a covert purpose. Recording the level of noise (e.g. the decibel level) will not normally capture private information and, therefore, does not require authorisation.
11. Recording sound (with a DAT recorder) on private premises could constitute intrusive surveillance, unless it is done overtly. For example, it will be possible to record if the noisemaker is warned that this will occur if the level of noise continues. Placing a stationary or mobile video camera outside a building to record anti social behaviour on residential estates will require prior authorisation.

**Further information**

12. Further guidance on CHIS can be found in the Home Office's Code of Practice on surveillance, at Appendix 7 and at:

[www.homeoffice.gov.uk/crimpol/crimreduc/regulation/codesofpractice.html](http://www.homeoffice.gov.uk/crimpol/crimreduc/regulation/codesofpractice.html)

## **H. Acquisition of Communications Data**

### **What is Communications Data?**

1. Communication data means any traffic or any information that is or has been sent by over a telecommunications system or postal system, together with information about the use of the system made by any person

### **Procedure**

2. There are two powers granted by S22 RIPA in respect of the acquisition of Communications Data from telecommunications and postal companies ("Communications Companies").
3. S22 (3) provides that an authorised person can authorise another person within the same relevant public authority to collect the data. This allows the local authority to collect the communications data themselves, i.e. if a Communications Service Provider is technically unable to collect the data, an authorisation under this section (Form C2) would permit the local authority to collect the communications data themselves.
4. In order to compel a Communications Service Provider to obtain and disclose, or just disclose Communications Data in their possession, a notice under S22 (4) RIPA (Form C4) must be issued. The sole grounds to permit the issuing of a S22 notice by a Permitted Local Authority is for the purposes of "preventing or detecting crime or of preventing disorder". The issuing of such a notice will be the more common of the two powers utilised, in that the Communications Service Provider will most probably have means of collating and providing the communications data requested.
5. Form C2 should only be used where the local authority is seeking to collect the information themselves, i.e. either to install its own monitoring system or using its own staff to obtain the information from the Communications Service Provider.
6. Form C4 should be used when the Communications Service Provider is being required to disclose or obtain and disclose the specified information.
7. Usage of Form C4 will be the more common form, in that the majority of the Communications Companies will have sufficient resources in place to allow them to collect the information following the service of a S22(4) Notice.
8. Once a notice has been issued, it must be sent to the Communications Service Provider. In issuing a notice, the Authorising Officer can authorise another person to liaise with the Communications Service Provider covered by the notice. Sample copies of an authorisation form and notice are set out below.
9. For Birmingham City Council Authorising Officers who have been duly authorised by the Corporate Director of Governance for the purposes of RIPA may sign the 'C' Forms. Copies of any 'C' Forms must, however, be provided to the Corporate Director of Governance within 1 week of signing the relevant Form.

## I. Authorisation Procedures

1. Directed surveillance and the use of a CHIS can only be lawfully carried out if properly authorised, and in strict accordance with the terms of the authorisation. **Appendix 2** provides flow charts of processes from application / consideration to recording of information and the storage / retention of data obtained.

### Authorising Officers

2. Forms can only be signed by Authorising Officers who hold a Certificate from the Corporate Director of Governance. Authorised posts are listed in **Appendix 1**. This Appendix will be kept up to date by the Corporate Director of Governance, and added to as needs require. If a Chief Officer wishes to add, delete or substitute a post, s/he must refer such request to the Corporate Director of Governance for consideration, as necessary. The Corporate Director of Governance has been duly authorised to add, delete or substitute posts listed in **Appendix 1**.
3. Authorisations under RIPA are separate from delegated authority to act under the Council's Scheme of Delegation and internal departmental Schemes of Delegation. All RIPA authorisations, save for authorisations to collect communications data under s22(3) are for specific investigations only, and must be reviewed, renewed or cancelled once the specific surveillance is complete or about to expire. **The authorisations do not lapse with time!** Authorisations to collect communications data under S22(3) have, as with S22 Notices, a life span of one month. However, they can be renewed by serving a new authorisation or notice for further months, within any time within the current life of the notice.

### Training Records

4. Appropriate training will be given (or approved) by the Corporate Director of Governance before Authorising Officers are certified to sign any RIPA Forms. A certificate of training will be provided to the individual and a Central Register of all those individuals who have undergone training (or a one-to-one meeting) with the Corporate Director of Governance on such matters will be kept by the Corporate Director of Governance.
5. If the Corporate Director of Governance feels that an Authorising Officer has not complied fully with the requirements of this Document, or the training provided to him, the Corporate Director of Governance is duly authorised to retract that Officer's certificate and authorisation until s/he has undertaken further approved training or a one-to-one meeting with the Corporate Director of Governance.

### Application Forms

6. Only the RIPA forms set out in this Document are permitted to be used. Any other forms used, will be rejected by the Authorising Officer and/or the Corporate Director of Governance.
7. **'A Forms' (Directed Surveillance), Guidance Note and Flowchart – See Appendix 3**

Form A 1	<b>Application</b> for Authority for Directed Surveillance
Form A 2	<b>Review</b> of Directed Surveillance Authority
Form A 3	<b>Renewal</b> of Directed Surveillance Authority
Form A 4	<b>Cancellation</b> of Directed Surveillance

(These forms have, subsequently, been used as the basis for the electronic database for applications for directed surveillance.)

8. **'B Forms' (CHIS), Guidance Note and Flowchart – See Appendix 4**
- |          |  |
|----------|--|
| Form B 1 | <b>Application</b> for Authority for Conduct and Use of a CHIS |
| Form B 2 | <b>Review</b> of Conduct and Use of a CHIS                     |
| Form B 3 | <b>Renewal</b> of Conduct and Use of a CHIS                    |
| Form B 4 | <b>Cancellation</b> of Conduct and Use of a CHIS               |

9. **Acquisition of Communications Data, Guidance Notes and Flowchart - See Appendix 5**

- |             |  |
|-------------|--|
| Form ACD 1  | <b>Application</b> form for Communications Data                                  |
| Form ACD 2  | <b>Application</b> for Communications Data SPOC Rejection Form                   |
| Form ACD 3  | SPOC <b>Log Sheet</b>  |
| Form ACD 4  | SPOC Officer <b>Report</b>   |
| Form ACD 5  | Designated Person's <b>Consideration</b> Form                                    |
| Form ACD 6  | <b>Authorisation</b> under Section 22(3) under the RIPA Act 2000                 |
| Form ACD 7  | <b>Notice</b> under Section 22(4) under the RIPA Act 2000                        |
| Form ACD 8  | <b>Cancellation</b> under Section 22(4)(8) under the RIPA Act 2000               |
| Form ACD 9  | <b>Cancellation</b> of Notice issued under Section 22(4)(8) of the RIPA Act 2000 |
| Form ACD 10 | <b>Cancellation</b> of Authorisation under Section 22(4)(8) of the RIPA Act 2000 |

**Grounds for Authorisation**

10. Directed Surveillance (A Forms); the Conduct and Use of the CHIS (B Forms) and/or disclosure of communications data notices (C Forms) can be authorised by the City Council only on the grounds of preventing or detecting crime or preventing disorder. No other grounds are available to local authorities.

**Assessing the Application Form**

11. Before an Authorising Officer signs a Form, **s/he must:-**
- (a) Be mindful of this Corporate Policy & Procedures Document, the Training provided by the Corporate Director of Governance and any other guidance issued, from time to time, by the Corporate Director of Governance on such matters;
  - (b) Satisfy his/herself that the RIPA authorisation is:-
    - (i) **in accordance with the law;**
    - (ii) **necessary** in the circumstances of the particular case on the grounds mentioned in paragraph 10 above; **and**
    - (iii) **proportionate** to what it seeks to achieve.
  - (c) In assessing whether or not the proposed surveillance is proportionate, consider whether there are any other non-intrusive, and if there are none, whether the proposed surveillance is no more than necessary to achieve the objective, as the **least intrusive method will be considered proportionate by the courts.**

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

For Covert Surveillance applications, the electronic database will provide a Unique Reference Number and authorising officers will be required to confirm review dates.

For Communications and CHIS applications, the authorising officer should:

- (e) Set a date for review of the authorisation and review on that date using the relevant form:
- (f) Allocate a Unique Reference Number (URN) for each form:-  

Year / Department / Number of Application
- (g) Ensure that any RIPA Departmental Register is duly completed, and that a copy of the RIPA Forms (and any review / renewal / cancellation of the same) is forwarded to the Corporate Director of Governance's Central Register, **within 1 week of the relevant authorisation, review, renewal, cancellation or rejection.**
- (h) In the case of notices relating to communications data, these will be kept by a SPoC designated by the Corporate Director of Governance and the Corporate Director of Governance will have access to such forms and as when required.
- (i) if unsure on any matter, obtain advice from the Corporate Director of Governance before signing any forms.

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

- 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 what is sought to be achieved;
  - (b) be satisfied that **appropriate arrangements** are in place for the management and oversight of the CHIS and this must address health and safety issues through a risk assessment;
  - (c) consider the likely degree of intrusion of all those potentially affected;
  - (d) consider any adverse impact on community confidence that may result from the use or conduct or the information obtained;
  - (e) ensure **records** contain particulars and are not available except on a need to know basis; and
  - (f) if unsure on any matter, obtain the advice from the Corporate Director of Governance before signing any forms.

### **Urgent Authorisations**

13. Urgent authorisations should not be necessary. In exceptional circumstances, however, urgent authorisations may be given orally if the time that would elapse before a written authorisation can be granted would be likely to endanger life or jeopardise the investigation or operation for which the authorisation was being given.
14. It will not be urgent where the need for authorisation has been neglected or is of the Officer's own making. All urgent authorisations must be promptly entered onto the corporate database at the earliest opportunity. Furthermore, a contemporary note of the case made by the applicant to the authorising officer to authorise the surveillance must be recorded as this represent an important aspect of the documentary evidence in relation to the case.
15. Urgent authorisations last for no more than 72 hours. They must be recorded in writing on the standard form on the electronic database as soon as practicable and the extra boxes on the form completed to explain why the urgent oral authorisation was necessary.

### **Duration**

16. The Form **must be reviewed in the time stated, renewed and / or cancelled** once it is no longer needed. The 'authorisation' to carry out/conduct the surveillance lasts for a maximum of 3 months (from authorisation) for Directed Surveillance, and 12 months (from authorisation) for a CHIS. However, whether the surveillance is carried out/conducted or not, in the relevant period, does not mean the 'authorisation' is 'spent'. In other words, **the Forms do not expire!** The forms have to be reviewed, renewed and / or cancelled (once they are no longer required)!
17. Notices/Authorities issued under S22 compelling disclosure of Communications Data are only valid for one month, but can be renewed for subsequent periods of one month, at any time.
18. Urgent oral authorisation, if not already ratified in a written authorisation, will cease to have effect after 72 hours, beginning with the time when the authorisation was granted.
19. Authorisations can be renewed in writing before the maximum period in the Authorisation has expired. 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. An Authorisation can not be renewed after it has expired. In such event, a fresh Authorisation will be necessary.
20. The renewal will begin on the day when the authorisation would have expired. In exceptional circumstances, renewals may be granted orally in urgent cases and last for a period of seventy-two hours.

## **J. Working With / Through Other Agencies**

1. When some other agency has been instructed on behalf of the City Council to undertake any action under RIPA, this Document and the Forms in it must be used (as per normal procedure) and the agency advised or kept informed, as necessary, of the various requirements. They must be made aware explicitly what they are authorised to do.
2. When some other agency (e.g. Police, Customs & Excise, Inland Revenue etc):-
  - (a) wish to use the City Council's resources (e.g. CCTV surveillance systems), that agency must use its own RIPA procedures and, before any Officer agrees to allow the City Council's resources to be used for the other agency's purposes, s/he must obtain a copy of that agency's RIPA form for the record (a copy of which must be passed to the Corporate Director of Governance for the Central Register) or relevant extracts from the same which are sufficient for the purposes of protecting the City Council and the use of its resources;
  - (b) wish to use the City Council's premises for their own RIPA action, and is expressly seeking assistance from the City Council, the Officer should, normally, co-operate with the same, unless there are security or other good operational or managerial reasons as to why the City Council's premises should not be used for the agency's activities. Suitable insurance or other appropriate indemnities may be sought, if necessary, from the other agency for the City Council's co-operation in the agent's RIPA operation. In such cases, however, the City Council's own RIPA forms should not be used as the City Council is only 'assisting' not being 'involved' in the RIPA activity of the external agency.
3. In terms of 2(a), if the Police or other Agency wish to use City Council resources for general surveillance, as opposed to specific RIPA operations, an appropriate letter requesting the proposed use, extent of remit, duration, who will be undertaking the general surveillance and the purpose of it must be obtained from the Police or other Agency before any City Council resources are made available for the proposed use.
4. **If in doubt, please consult with the Corporate Director of Governance at the earliest opportunity.**

## **K. Record Management**

1. **The City Council must keep a detailed record of all Authorisations, Reviews, Renewals, Cancellations and rejections in Departments and a Central Register of all Authorisation Forms will be maintained and monitored by the Corporate Director of Governance (in relation to Forms A and B). In relation to Forms C, a SPoC designated by the Corporate Director of Governance will retain the forms and the Corporate Director of Governance will have access to Form C's as and when required.**

2. **Records maintained in the Department**

The City Council will retain records for a period of at least three years from the ending of the Authorisation. The Office of the Surveillance Commissioners (OSC) can audit/review the City Council's policies and procedures, and individual Authorisations, Reviews, Renewals, Cancellations and rejections. The database allows for the storage and management of applications and includes:

- a copy of the Forms together with any supplementary documentation and notification of the approval given by the Authorising Officer;
- a record of the period over which the surveillance has taken place;
- the frequency of reviews prescribed by the Authorising Officer;
- a record of the result of each review of the authorisation;
- a copy of any renewal of an authorisation, together with the supporting documentation submitted when the renewal was requested;
- the date and time when any instruction was given by the Authorising Officer;
- the Unique Reference Number for the authorisation (URN).

**Central Register maintained by the Corporate Director of Governance**

3. For Directed Surveillance, the electronic database constitutes the Central Register and the database is administered by the Corporate Information Governance Team, who report to the Corporate Director of Governance. For CHIS applications, Authorising Officers must forward details of each Form B to the Corporate Director of Governance for the Central Register, within 1 week of the Authorisation, Review, Renewal, Cancellation or rejection. The Corporate Director of Governance will monitor the same and give appropriate guidance, from time to time, or amend this Document, as necessary. Forms C will be sent to the SPoC designated by the Corporate Director of Governance.

## **L. Concluding Remarks of the Corporate Director of Governance**

1. Where there is an interference with the right to respect for private life and family guaranteed under Article 8 of the European Convention on Human Rights, and where there is no other source of lawful authority for the interference, or if it is held not to be necessary or proportionate to the circumstances, the consequences of not obtaining or following the correct authorisation procedure set out in RIPA and this Document, may be that the action (and the evidence obtained) will be held to be unlawful by the Courts pursuant to Section 6 of the Human Rights Act 1998.
2. Obtaining an authorisation under RIPA and following this Document, will ensure, therefore, that the action is carried out in accordance with the law and subject to stringent safeguards against abuse of anyone's human rights.
3. **Authorising Officers will be suitably trained and they must exercise their minds every time they are asked to consider a Form. They must never sign or rubber stamp Form(s) without thinking about their own personal and the City Council's responsibilities.**
4. **Any boxes not needed on the Form(s) must be clearly marked as being 'NOT APPLICABLE', 'N/A' or a line put through the same.** Great care must also be taken to ensure accurate information is used and is inserted in the correct boxes. Reasons for any refusal of an application must also be kept on the form and the form retained for future audits.
5. For further advice and assistance on RIPA, please contact the City Council's Corporate Director of Governance (who is also the Monitoring Officer). Details are provided on the front of this Document.

## **RIPA AUTHORISING OFFICERS**

### **Chief Executive**

David Tatlow Trained: 17/3/03	Director of Legal Services
<b>Jane Robson</b> Trained: 17/3/03	Assistant Director (Adults & Children) Legal & Democratic Services
John Wynn Trained: 17/3/03 & 28/6/05	Assistant Director (Public Law & Property) Legal & Democratic Services
Jacqui Kennedy (training given by John Martin)	Director of Regulatory Services
<b>Andy Albon</b> Trained: 17/3/03	Director of Corporate Human Resources
Jim Wilkinson Trained: 20/6/03	Assistant Director (Audit and Risk Management)
John Turner Trained: 17/3/03	Business Manager, Birmingham Audit
Laeq Beg Training: 17/3/03 and 4/2/09	Operations Manager, Benefit Counter Fraud Team, Birmingham Audit
Jon Warlow Trained 16/07/09	Director of Corporate Finance
Chris Neville Trained 16/07/09	Head of Trading Standards

### **Children, Young People and Families**

Sam Hulson Trained: 4/2/09	HR Business Partner for Schools
-------------------------------	---------------------------------

### **Housing & Constituencies**

Ann M Brookes Trained: 8/04/08	Governance & Facilities Manager, HOUSING
-----------------------------------	--

### **Development**

John Blakemore Trained: 6/10/08	Director of Highways Resilience
Trevor Haynes Trained: 5/7/04	<b>Assistant Director – Building and Consultancy Services</b>
Steve Vickers Trained: 17/3/03	General Manager, Urban Design
Richard Goulborn Trained 16/07/09	Head of Service Development

### **Environment & Culture**

Sharon Lea Trained: 17/3/03	Acting Strategic Director of Environment & Culture
Penny Smith Trained: 28/6/05	Assistant Director of Leisure & Support Services
Kevin Mitchell Trained: 8/4/08	Assistant Director of Fleet & Waste Management

### **Adults & Communities**

Steve Wise Trained: 6/3/06	Project Director, Transformation for Adults & Communities
-------------------------------	---

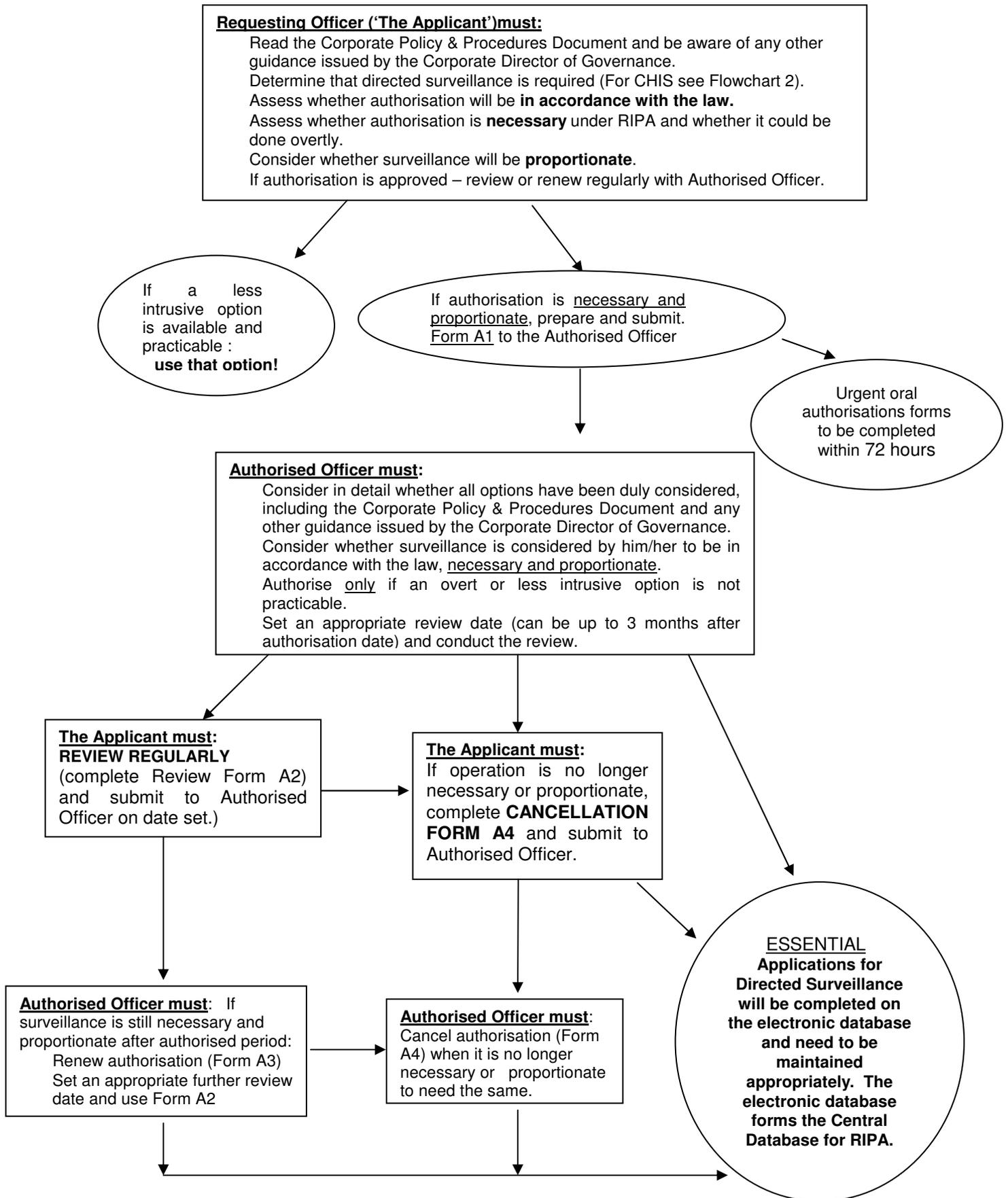
<b>Single Point of Contact (SPoC)</b>	
Huw Jones	Team Leader, Trading Standards

**Last Updated: 8 April 2011**

**IMPORTANT NOTES:**

- A.** Even if a post is identified in the above list the persons currently employed in such posts are not authorised to sign RIPA Forms (including a review, renewal or cancellation) unless s/he has been certified by the Corporate Director of Governance to do so.
- B.** Only the Chief Executive and the Corporate Director of Governance are authorised to sign Forms relating to Juvenile Sources and Vulnerable Individuals (see Section **G** of this Document), or where there is any possibility of confidential information being obtained.
- C.** If a Chief Officer wishes to add, delete or substitute a post, s/he must refer such request to the Corporate Director of Governance for consideration, as necessary.
- D.** If in doubt, ask the Corporate Director of Governance BEFORE any directed surveillance and/or CHIS is Authorised, Reviewed, Renewed, Cancelled or rejected.

# RIPA FLOW CHART 1 : DIRECTED SURVEILLANCE



**NB: If in doubt, ask the Corporate Director of Governance BEFORE any directed surveillance and/or CHIS is Authorised, Reviewed, Renewed, Cancelled, or rejected. Chief Officers will designate one of their staff to be a Departmental Co-ordinator for the purpose of RIPA and advise the Corporate Director of Governance, accordingly.**

## RIPA A FORMS: DIRECTED SURVEILLANCE

**Form A1** : Application for authorisation to carry out directed surveillance.

**Form A2** : Review of Form A1.

**Form A3** : Application for Renewal of Form A1.

**Form A4** : Cancellation of Form A1.

**NB: If in doubt, ask the Corporate Director of Governance BEFORE any directed surveillance and/or CHIS is authorised, reviewed, renewed, cancelled or rejected.**

# BIRMINGHAM CITY COUNCIL

**STRICTLY PRIVATE  
& CONFIDENTIAL**

## **FORM A1: APPLICATION FOR AUTHORISATION TO CARRY OUT DIRECTED SURVEILLANCE**

### **PART II OF THE REGULATION OF INVESTIGATORY POWERS ACT 2000 (RIPA)**

**Guidance Note:**

1. After 1 April 2003, only Authorising Officers who have been certified by the Corporate Director of Governance will be allowed to sign RIPA Forms.
2. Applicants and Authorising Officers must comply, in full, with the Act and the City Council's Corporate Policy & Procedures Document and any other guidance issued, from time to time, by the Corporate Director of Governance. If in doubt, contact the Corporate Director of Governance, Mirza Ahmad, MBA, LL.M Barrister, Ingleby House, 11-14 Cannon Street, Birmingham B2 5EN. Tel: 0121 303 9991. Fax: 0121 303 1312. E-mail: mirza\_ahmad@birmingham.gov.uk
3. Copy of completed forms must be sent (once authorised or rejected) to the Corporate Director of Governance within 1 week of the authorisation, review, renewal, cancellation or rejection for the Central Register.
4. All boxes in this form must be completed. NOT APPLICABLE, N/A or lines must be put through irrelevant boxes.

<b>Subject of Surveillance</b> <i>(including full address)</i>		Unique Reference Number (URN):	Year/Dept/Number
---	--	-----------------------------------	------------------

### **SECTION 1 (to be completed by the Applicant)**

<b>Name of Applicant</b>		<b>Unit/Division</b>	
<b>Full Address</b>			
<b>Contact Details</b>			
<b>Investigation/Operation Name (if applicable)</b>			

**Details of application:**

**1. Give name / job title of Authorised Officer:**

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

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

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

- Name:
- Address:
- DOB:
- Other known / relevant information:

**5. Explain the information that is desired to obtain as a result of the directed surveillance:**

**6. Explain why directed surveillance is NECESSARY in this particular case:**

**NB: UNDER SECTION 28 OF RIPA, THE ONLY GROUND AVAILABLE TO THE COUNCIL IS “FOR THE PURPOSE OF PREVENTING OR DETECTING CRIME OR OF PREVENTING DISORDER”. THIS APPLICATION MUST BE REJECTED, IF THIS GROUND IS NOT RELEVANT TO THE PROPOSED SURVEILLANCE.**

**7. Supply details of any potential COLLATERAL INTRUSION and why the intrusion is unavoidable:  
(Also describe precautions to MINIMISE collateral intrusion)**

**8. Explain why the directed surveillance is PROPORTIONATE to what it seeks to achieve. How intrusive might it be or the subject of surveillance or on others? And why is this intrusion outweighed by the need for surveillance in operational terms or can the evidence be obtained by any other means?**

**9. Confidential information (e.g. confidential legal privilege, personal information and journalistic material)**

INDICATE THE LIKELIHOOD OF ACQUIRING ANY CONFIDENTIAL INFORMATION

**10. Applicant's Details.**

Name (print)

Tel No:

Job Title

Date

Signature

**11. Anticipated Start Date Time**

Date:

Time:

**SECTION 2 (To be completed by the Authorised Officer)**

**12. Authorised Officer's Statement must spell out the "5 W's" – Who; What; Where; Why and How.**

**1. I hereby authorise as follows:**

*Who is authorised to conduct surveillance:*

*What is authorised for the surveillance:*

*Where is it to take place and for how long:*

*Why is it being authorised:*

*How will the surveillance be conducted:*

2. This written authorisation will cease to have effect at the end of a period of 3 months unless renewed (see separate form for renewals).
3. The Applicant and the Authorised Officer will jointly review this authorisation on the date below to see whether the authorisation should continue, be renewed or cancelled.

--

**13. Authorised Officer's statement explaining why in his / her view the directed surveillance is necessary and proportionate. This box must be completed and both aspects must be addressed.**

Why is it necessary?

Why is it proportionate?

**14. Confidential Information Authorisation. Supply details demonstrating compliance with Home Office Codes of Practice relating to this issue.**

--

**Expiry of Authorisation (3 months from date / time of Authorisation unless stated here):**

**Date of first review:**

**Date of subsequent reviews of this Authorisation:**

**Authorised Officer's Name:**

**Job Title:**

**Signature:**

**Date / Time:**

**16. Urgent Authorisation: Authorised Officer to explain why s/he considered the case so urgent that an oral, instead of a written, authorisation was given.**

--

**URGENT AUTHORISATION EXPIRY DATE / TIME : (72 HOURS) AFTER ORAL AUTHORISATION).**



# BIRMINGHAM CITY COUNCIL

**STRICTLY PRIVATE  
& CONFIDENTIAL**

## FORM A2: REVIEW OF A DIRECTED SURVEILLANCE AUTHORISATION

### PART II OF THE REGULATION OF INVESTIGATORY POWERS ACT 2000 (RIPA)

**Guidance Note:**

1. After 1 April 2003, only Authorising Officers who have been certified by the Corporate Director of Governance will be allowed to sign RIPA Forms.
2. Applicants and Authorising Officers must comply, in full, with the Act and the City Council's Corporate Policy & Procedures Document and any other guidance issued, from time to time, by the Corporate Director of Governance. If in doubt, contact the Corporate Director of Governance, Mirza Ahmad, MBA, LL.M Barrister, Ingleby House, 11-14 Cannon Street, Birmingham B2 5EN. Tel: 0121 303 9991. Fax: 0121 303 1312.  
E-mail: mirza\_ahmad@birmingham.gov.uk
3. Copy of completed forms must be sent (once authorised or rejected) to the Corporate Director of Governance within 1 week of the authorisation, review, renewal, cancellation or rejection for the Central Register.

**SECTION 1 (To be completed by the Applicant)**

<b>Subject of Surveillance:</b>		<b>Unique Reference Number (URN):</b>	/ /
			Year / Dept / Number

<b>Name of Applicant:</b>		<b>Unit/Division:</b>			
<b>Full Address:</b>					
<b>Contact Details:</b>					
<b>Operation Name:</b>		<b>Form A1 URN</b>	(Dept)	(Year)	(Number)
<b>Date of authorisation or last renewal:</b>		<b>Expiry date of authorisation or last renewal:</b>			
		<b>Form A2 URN</b>			

**Details of review:**

<b>1. Review number and dates of any current and previous reviews:</b>	
<b>Review Number:</b>	<b>Date:</b>

<b>2. Summary of the investigation/operation to date, including what private information has been obtained and the value of the information so far obtained:</b>

<b>3. Detail the reasons why it is NECESSARY to continue with the directed surveillance:</b>

<b>4. Explain how the proposed activity is still PROPORTIONATE to what it seeks to achieve:</b>

<b>5. Detail any incidents of collateral intrusion and the likelihood of any further incidents of collateral intrusions occurring:</b>

**6. Give details of any confidential information acquired or accessed and the likelihood of acquiring confidential information:**

--

**7. Applicant's Details:**

Name (Print):

Tel No:

Job Title:

Date:

Signature:

**SECTION 2 (To be completed by the Authorised Officer)**

**8. Authorised Officer's Comments, including whether or not the directed surveillance should continue:**

--

**9. Authorised Officer's Statement:**

I hereby agree that the directed surveillance, as detailed above, should [continue until its next review] [be cancelled immediately].

Name (Print):

Job Title:

Signature:

Date:

**1. Date of next review:**

--

**NB: A copy of this form, once it has been authorised or rejected must be sent to the Corporate Director of Governance within 1 week of the authorisation or rejection for placing the Birmingham City Council's central register.**

# BIRMINGHAM CITY COUNCIL

**STRICTLY PRIVATE  
& CONFIDENTIAL**

## **FORM A3: APPLICATION FOR RENEWAL OF A DIRECTED SURVEILLANCE AUTHORISATION**

**(Please attach a copy of the original authorisation)**

### **PART II OF THE REGULATION OF INVESTIGATORY POWERS ACT 2000 (RIPA)**

**Guidance Note:**

1. After 1 April 2003, only Authorising Officers who have been certified by the Corporate Director of Governance will be allowed to sign RIPA Forms.
2. Applicants and Authorising Officers must comply, in full, with the Act and the City Council's Corporate Policy & Procedures Document and any other guidance issued, from time to time, by the Corporate Director of Governance. If in doubt, contact the Corporate Director of Governance, Mirza Ahmad, MBA, LL.M Barrister, Ingleby House, 11-14 Cannon Street, Birmingham B2 5EN. Tel: 0121 303 9991. Fax: 0121 303 1312. E-mail: mirza\_ahmad@birmingham.gov.uk
3. Copy of completed forms must be sent (once authorised or rejected) to the Corporate Director of Governance within 1 week of the authorisation, review, renewal, cancellation or rejection for the Central Register.
4. All boxes in this form must be completed. NOT APPLICABLE, N/A or lines must be put through irrelevant boxes.

#### **SECTION 1 (To be completed by the Applicant)**

<b>Subject of Surveillance:</b>		<b>Unique Reference Number (URN):</b>	/ /
			Year/ Dept / Number

<b>Name of Applicant:</b>		<b>Unit/ Division:</b>	
<b>Full Address:</b>			
<b>Contact Details:</b>			
<b>Investigation/ Operation Name: (if applicable)</b>			
<b>Renewal Number</b>			

**Details of renewal:**

<b>2. Renewal numbers and dates of any current and previous renewals:</b>	
<b>Renewal Number</b>	<b>Date:</b>

**3. Detail any significant changes to the information provided in the original authorisation, as it applies at the time of the renewal:**

**4. Detail the reasons why it is NECESSARY to continue with the directed surveillance:**

**5. Detail why the directed surveillance is still PROPORTIONATE to what it seeks to achieve:**

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

--

**7. Give details of the results of the regular reviews of the investigation or operation:**

--

**8. Applicant's Details:**

**Name (Print):**

**Tel No:**

**Job Title:**

**Date:**

**Signature:**

**SECTION 2 (To be completed by the Authorised Officer)**

**9. Authorised Officer's Comments: This box must be completed to indicate why the renewal (if agreed) is necessary and proportionate.**

--

**10. Authorised Officer's Statement:**

I hereby authorise [or reject] the renewal of the directed surveillance operation as detailed above. The renewal (if authorised) will last for 3 months unless renewed in writing.

This renewal will be reviewed frequently to assess the need for the authorisation to continue.

**Name (Print):** ..... **Job Title:**

**Signature:** ..... **Date:**

**Renewal Time:** ..... **Date:**  
**From:**

<b>Date of first review:</b>	
<b>Date of subsequent reviews of this authorisation:</b>	

**NB: A copy of this form, once it has been authorised or rejected must be sent to the Corporate Director of Governance within 1 week of the authorisation or rejection for placing the Birmingham City Council's central register.**



# BIRMINGHAM CITY COUNCIL

<b>STRICTLY PRIVATE &amp; CONFIDENTIAL</b>
--

## FORM A4: CANCELLATION OF A DIRECTED SURVEILLANCE AUTHORISATION

### PART II OF THE REGULATION OF INVESTIGATORY POWERS ACT (RIPA) 2000

**Guidance Note:**

1. After 1 April 2003, only Authorising Officers who have been certified by the Corporate Director of Governance will be allowed to sign RIPA Forms.
2. Applicants and Authorising Officers must comply, in full, with the Act and the City Council's Corporate Policy & Procedures Document and any other guidance issued, from time to time, by the Corporate Director of Governance. If in doubt, contact the Corporate Director of Governance, Mirza Ahmad, MBA, LL.M Barrister, Ingleby House, 11-14 Cannon Street, Birmingham B2 5EN. Tel: 0121 303 9991. Fax: 0121 303 1312. E-mail: mirza\_ahmad@birmingham.gov.uk
3. Copy of completed forms must be sent (once authorised or rejected) to the Corporate Director of Governance within 1 week of the authorisation, review, renewal, cancellation or rejection for the Central Register.

**SECTION 1 (To be completed by the Applicant)**

<b>Subject of Surveillance:</b>		<b>Unique Reference Number (URN):</b>	/ /
			Year / Dept / Number

<b>Name of Applicant:</b>		<b>Unit/Division:</b>	
<b>Full Address:</b>			
<b>Contact Details:</b>			
<b>Investigation /Operation Name: (if applicable)</b>			
<b>Form A1 URN:</b>		<b>Form A 2 URN:</b>	<b>Form A3 URN:</b>

**Details of cancellation:**

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

--

**2. Explain the value of surveillance in the operation:**

--

**SECTION 2 (To be completed by the Authorised Officer)**

**3. Authorised Officer's statement:**

I hereby authorise the cancellation of the directed surveillance as detailed above.

**Name (Print):** .....

**Job Title:** .....

**Signature:** .....

**Date:** .....

**4. Time and Date of when the Authorised Officer instructed the surveillance to cease:**

<b>Date:</b>		<b>Time:</b>	
--------------	--	--------------	--

**5. Authorisation cancelled:**

**Date:**

**Time:**

**NB: A copy of this form, once it has been authorised or rejected must be sent to the Corporate Director of Governance within 1 week of the authorisation or rejection for placing the Birmingham City Council's central register.**

## RIPA B FORMS: COVERT HUMAN INTELLIGENCE SOURCE (CHIS)

### Additional Notes on CHIS (This is an extract from Home Office Code of Practice on CHIS)

#### MANAGEMENT OF SOURCES

##### Tasking

1. Tasking is the assignment given to the source by the persons defined at sections 29(5)(a) and (b) of the 2000 Act, asking him to obtain information, to 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 source is required prior to any tasking where such tasking requires the source to establish or maintain a personal or other relationship for a covert purpose.
2. The person referred to in section 29(5)(a) of the 2000 Act will have day to day responsibility for:
  - dealing with the source on behalf of the authority concerned;
  - directing the day to day activities of the source;
  - recording the information supplied by the source; and
  - monitoring the source's security and welfare;
3. The person referred to in section 29(5)(b) of the 2000 Act will be responsible for the general oversight of the use of the source.
4. In some instances, the tasking given to a person will not require the source to establish a personal or other relationship for a covert purpose. For example a source may be tasked with finding out purely factual information about the layout of commercial premises.
5. It is not the intention that authorisations be drawn so narrowly that a separate authorisation is required each time the source is tasked. Rather, an authorisation might cover, in broad terms, the nature of the source's task. If this changes, then a new authorisation may need to be sought.
6. It is difficult to predict exactly what might occur each time a meeting with a source takes place, or the source meets the subject of an investigation. There may be occasions when unforeseen action or undertakings occur. When this happens, the occurrence must be recorded as soon as practicable after the event and, if the existing authorisation is insufficient it should either be updated and re-authorised (for minor amendments only) or it should be cancelled and a new authorisation should be obtained before any further such action is carried out.
7. Similarly where it is intended to task a source in a new way or significantly greater way than previously identified, the persons defined at section 29(5)(a) or (b) of the 2000 Act must refer the proposed tasking to the authorising officer, who should consider whether a separate authorisation is required. This should be done in advance of any tasking and the details of such referrals must be recorded.

## Management responsibility

8. Public authorities should ensure that arrangements are in place for the proper oversight and management of sources, including appointing individual officers as defined in section 29(5)(a) and (b) of the 2000 Act for each source.
9. The person responsible for the day-to-day contact between the public authority and the source will usually be of a rank or position below that of the Authorising Officer.
10. In cases where the authorisation is for the use or conduct of a source whose activities benefit more than a single public authority, responsibilities for the management and oversight of that source may be taken up by one authority or can be split between the authorities.

## Security and welfare

11. Any public authority deploying a source should take into account the safety and welfare of that source, when carrying out actions in relation to an authorisation or tasking, and to foreseeable consequences to others of that tasking. Before authorising the use or conduct of a source, the Authorising Officer should ensure that a risk assessment is carried out to determine the risk to the source of any tasking and the likely consequences should the role of the source become known. The ongoing security and welfare of the source, after the cancellation of the authorisation, should also be considered at the outset.
12. The person defined at section 29(5)(a) of the 2000 Act is responsible for bringing to the attention of the person defined at section 29(5)(b) of the 2000 Act any concerns about the personal circumstances of the source, insofar as they might affect:
  - the validity of the risk assessment
  - the conduct of the source, and
  - the safety and welfare of the source.
13. Where deemed appropriate, concerns, about such matters must be considered by the authorising officer, and a decision taken on whether or not to allow the authorisation to continue.

**Form B1** : **Application** for authorisation of the **Use** or **Conduct** of a Covert Human Intelligence Source (CHIS).

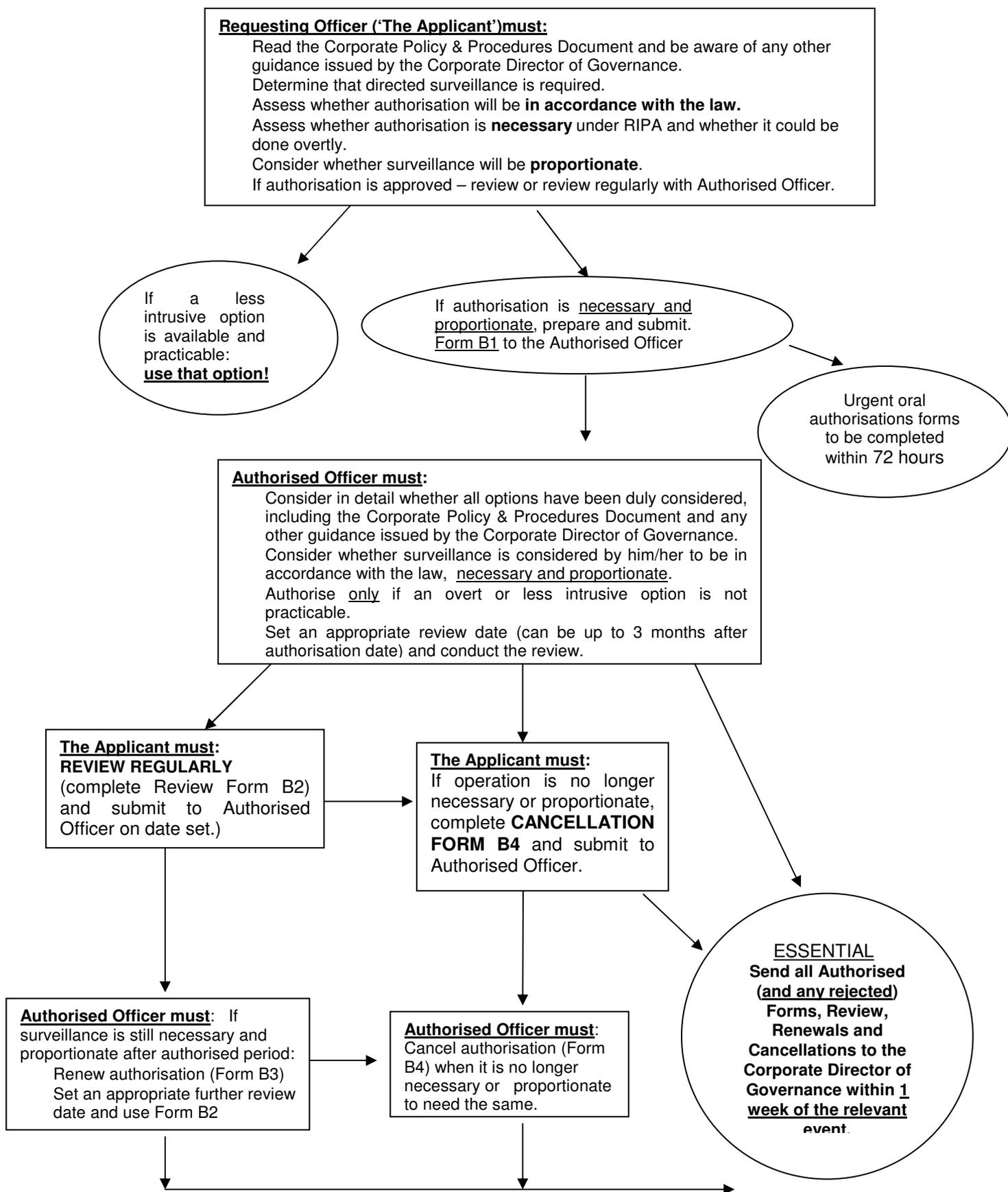
**Form B2** : **Review** of Form B1.

**Form B3** : Application for **Renewal** of Form B 1.

**Form B4** : **Cancellation** of Form B1

**NB: If in doubt, ask the Corporate Director of Governance BEFORE any directed surveillance and/or CHIS is authorised, reviewed, renewed, rejected or cancelled.**

## RIPA FLOW CHART 2: CHIS



**NB: If in doubt, ask the Corporate Director of Governance BEFORE any directed surveillance and/or CHIS is Authorised, Reviewed, Renewed, Cancelled, or rejected. Chief Officers will designate one of their staff to be a Departmental Co-ordinator for the purpose of RIPA and advise the Corporate Director of Governance, accordingly.**



# BIRMINGHAM CITY COUNCIL

**STRICTLY PRIVATE  
& CONFIDENTIAL**

## **FORM B1: APPLICATION FOR AUTHORISATION OF THE USE OR CONDUCT OF A COVERT HUMAN INTELLIGENCE SOURCE (CHIS)**

### **PART II OF THE REGULATION OF INVESTIGATORY POWERS ACT 2000 (RIPA)**

**Guidance Note:**

1. After 1 April 2003, only Authorising Officers who have been certified by the Corporate Director of Governance will be allowed to sign RIPA Forms.
2. Applicants and Authorising Officers must comply, in full, with the Act and the City Council's Corporate Policy & Procedures Document and any other guidance issued, from time to time, by the Corporate Director of Governance. If in doubt, contact the Corporate Director of Governance, Mirza Ahmad, MBA, LL.M Barrister, Ingleby House, 11-14 Cannon Street, Birmingham B2 5EN. Tel: 0121 303 9991. Fax: 0121 303 1312. E-mail: mirza\_ahmad@birmingham.gov.uk
3. Copy of completed forms must be sent (once authorised or rejected) to the Corporate Director of Governance within 1 week of the authorisation, review, renewal, cancellation or rejection for the Central Register.
4. All boxes in this form must be completed. NOT APPLICABLE (N/A) or lines must be put through irrelevant boxes.

#### **SECTION 1 (To be completed by the Applicant)**

<b>Subject of Surveillance:</b>		<b>Unique Reference Number (URN):</b>	/ /
			Year / Dept / Number

<b>Name of Applicant:</b>		<b>Unit/Division:</b>	
<b>Full Address:</b>			
<b>Contact Details:</b>			
<b>Investigation /Operation Name: (if applicable)</b>			

**Details of application:**

**1. Give job title of Authorised Officer:**

--

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

--

**3. Describe in detail the purpose of which the source will be tasked or deployed.**

--

**4. Describe in detail what the source will be tasked to do or how the source will be deployed:**

--

**5. Identify whether the grounds for any action is NECESSARY under section 29(3) of RIPA.**

--

**6. Explain why conduct or use of a covert human intelligence source (CHIS) is NECESSARY in this particular case:**

--

**6. Where a specific investigation or operation is involved, details of that investigation or operation:**

--

**7. Supply details of any potential Collateral Intrusion and why the intrusion is unavoidable. Also include a plan to minimise collateral intrusion:**

--

**8. Explain why the conduct or use of a source is PROPORTIONATE to what it seeks to achieve. How intrusive might it be on the subject(s) of surveillance or on others? And why is this intrusion outweighed by the need for a source in operational terms or can the evidence be obtained by any other lesser / intrusive means?**

--

**9. Confidential Information (e.g. confidential legal privilege, personal information or journalistic material):**

**INDICATE THE LIKELIHOOD OF ACQUIRING ANY CONFIDENTIAL INFORMATION.**

**10. Details of the risk assessment on the security and welfare of using the source:**

**11. Anticipated Start:**

**Date:**

**Time:**

**12. Applicant's Details:**

**Name  
(print):**

**Tel No:**

**Job Title:**

**Date:**

**Signature:**

**SECTION 2 (To completed by the Authorised Officer)**

**13. Authorising Officer's Comments: This box must be completed. Spell out the "5W's" – who, what, where, when, why and how:**

Who is the CHIS and who is the subject of surveillance:

What is the surveillance for?

When will be surveillance take place?

Why is the surveillance necessary?

How will the surveillance be undertaken?

**14. Explain why you believe the conduct or use of the source is necessary. Explain why you believe the conduct or use of the source to be proportionate to what is sought to be achieved by carrying it out.**

**15. Confidential Information Authorisation. Supply details demonstrating compliance with Home Office Codes of Practice relating to this issue:**

**16. Authorising Officer's Statement:**

1. I hereby [authorise] [reject] the directed surveillance operation detailed above. If authorised, this written authorisation will cease to have effect if not actioned within a period of 3 months.
2. The Applicant will review this authorisation on \_\_\_\_\_ to see whether the authorisation should be continued, further reviewed, renewed or cancelled.
3. The Applicant will take appropriate action on \_\_\_\_\_ to seek the review, renewal or cancellation of this authorisation from the Authorised Officer.

<b>Name (Print):</b>		<b>Job Title:</b>	
<b>Signature:</b>		<b>Date / time:</b>	
<b>Start date / time:</b>			
<b>17. Date of first review:</b>			
<b>18. Date of subsequent reviews of this authorisation:</b>			

**URGENT AUTHORISATION**

**19. Urgent Authorisation. Authorised Officer to explain why s/he considered the case so urgent that an oral, instead of a written authorisation, was given:**

**Name (Print):** .....

**Job Title:** .....

**Signature:**

**Date/Time:**

**NB: Oral authorisation only lasts up to 72 hours! A written form must be completed by such deadline.**

**NB: A copy of this Form, once it has been authorised together with a copy of the original authorisation must be sent to the Corporate Director of Governance within 1 week of signing for placing on the Birmingham City Council's central register**

# BIRMINGHAM CITY COUNCIL

**STRICTLY PRIVATE  
& CONFIDENTIAL**

## **FORM B2: REVIEW OF A COVERT HUMAN INTELLIGENCE SOURCE (CHIS) AUTHORISATION**

### **PART II OF THE REGULATION OF INVESTIGATORY POWERS ACT 2000 (RIPA)**

**Guidance Note:**

1. After 1 April 2003, only Authorising Officers who have been certified by the Corporate Director of Governance will be allowed to sign RIPA Forms.
2. Applicants and Authorising Officers must comply, in full, with the Act and the City Council's Corporate Policy & Procedures Document and any other guidance issued, from time to time, by the Corporate Director of Governance. If in doubt, contact the Corporate Director of Governance, Mirza Ahmad, MBA, LL.M Barrister, Ingleby House, 11-14 Cannon Street, Birmingham B2 5EN. Tel: 0121 303 9991. Fax: 0121 303 1312. E-mail: mirza\_ahmad@birmingham.gov.uk
3. Copy of completed forms must be sent (once authorised or rejected) to the Corporate Director of Governance within 1 week of the authorisation, review, renewal, cancellation or rejection for the Central Register.

**SECTION 1 (To be completed by the Applicant)**

<b>Subject of Surveillance:</b>		<b>Unique Reference Number (URN):</b>	/ /
			Year / Dept / Number

<b>Name of Applicant:</b>		<b>Unit/Division:</b>	
<b>Full Address:</b>			
<b>Contact Details:</b>			
<b>Operation Name:</b>		<b>Form B1 URN:</b>	
<b>Date of authorisation or last renewal:</b>		<b>Expiry date of authorisation or last renewal:</b>	
		<b>Form B3 URN:</b>	

**Details of review:**

<b>1. Review number and dates of any current and previous reviews:</b>	
<b>Review Number:</b>	<b>Date:</b>

<b>2. Summary of the investigation/operation to date, including what information has been obtained and the value of the information so far obtained:</b>

<b>3. Detail the reasons why it is NECESSARY to continue with using a Covert Human Intelligence Source:</b>

<b>4. Explain how the proposed activity is still PROPORTIONATE to what it seeks to achieve:</b>

**5. Detail any incidents of collateral intrusion and the likelihood of any further incidents of collateral intrusions occurring:**

--

**6. Give details of any confidential information acquired or accessed and the likelihood of acquiring confidential information:**

--

**7. Give details of the review of the risk assessment on the security and welfare of using the source:**

--

**8. Applicant's Details:**

<b>Name (Print):</b>		<b>Tel No:</b>	
<b>Job Title:</b>		<b>Date:</b>	
<b>Signature:</b>			

**SECTION 2 (To be completed by the Authorised Officer)**

**9. Authorised Officer's Comments, including whether or not the use or conduct of the source should continue:**

--

**10. Authorised Officer's Statement:**

I hereby agree that the use or conduct of the source as detailed above should [continue until its next review][or be cancelled immediately].

Name (Print): ..... Job Title:

Signature: ..... Date:

Date of next review:

**NB: A copy of this Form, once it has been authorised together with a copy of the original authorisation must be sent to the Corporate Director of Governance within 1 week of signing for placing on the Birmingham City Council's central register**

# BIRMINGHAM CITY COUNCIL

**STRICTLY PRIVATE  
& CONFIDENTIAL**

## **FORM B3: APPLICATION FOR RENEWAL OF A COVERT HUMAN INTELLIGENCE SOURCE (CHIS) AUTHORISATION**

(please attach the original authorisation)

### **PART II OF THE REGULATION OF INVESTIGATORY POWERS ACT 2000 (RIPA)**

**Guidance Note:**

1. After 1 April 2003, only Authorising Officers who have been certified by the Corporate Director of Governance will be allowed to sign RIPA Forms.
2. Applicants and Authorising Officers must comply, in full, with the Act and the City Council's Corporate Policy & Procedures Document and any other guidance issued, from time to time, by the Corporate Director of Governance. If in doubt, contact the Corporate Director of Governance, Mirza Ahmad, MBA, LL.M Barrister, Ingleby House, 11-14 Cannon Street, Birmingham B2 5EN. Tel: 0121 303 9991. Fax: 0121 303 1312. E-mail: mirza\_ahmad@birmingham.gov.uk
3. Copy of completed forms must be sent (once authorised or rejected) to the Corporate Director of Governance within 1 week of the authorisation, review, renewal, cancellation or rejection for the Central Register.
4. All boxes in this form must be completed. NOT APPLICABLE, N/A or lines must be put through irrelevant boxes.

**SECTION 1 (To be completed by the Applicant)**

<b>Subject of Surveillance:</b>		<b>Unique Reference Number (URN):</b>	/ /
			Year / Dept / Number

<b>Name of Applicant:</b>		<b>Unit/Division:</b>	
<b>Full Address:</b>			
<b>Contact Details:</b>			
<b>Investigation /Operation Name: (if applicable)</b>			
<b>Renewal relates to Form B1:</b>	(Year)	(Dept)	(Number)

**Details of renewal:**

<b>1. Renewal numbers and dates of any current and previous renewals:</b>	
<b>Renewal Number:</b>	<b>Date:</b>

<b>2. Detail any significant changes to the information in the previous authorisation:</b>

<b>3. Detail any significant changes to the information as listed in the original authorisation as it applies at the time of the renewal:</b>

<b>4. Detail why it is NECESSARY to continue with the authorisation, including details of any tasking given to the source:</b>

**5. Detail why the use or conduct of the source is still PROPORTIONATE to what it seeks to achieve:**

**6. Detail the use made of the source in the period since the grant of authorisation or, as the case may be, latest renewal of the authorisation:**

**7. List the tasks given to the source during that period and the information obtained from the conduct or use of the source:**

**8. Detail the results of regular reviews of the use of the source:**

**9. Give details of the review of the risk assessment on the security and welfare of using the source:**

10. Applicant's Details:			
Name (Print):		Tel No:	
Job Title:		Date:	
Signature:			

**SECTION 2 (To be completed by the Authorised Officer)**

<b>11. Authorised Officer's Comments:</b> <u>This box must be completed to show why it is (or is not) necessary and proportionate to continue the surveillance / operation.</u>

12. Authorised Officer's Statement:	
<p>I hereby [authorise] [reject] the renewal of the conduct/use of the source as detailed above. If renewed, the renewal will last for 12 months unless further renewed in writing.</p> <p>This authorisation will be reviewed frequently to assess the need for the authorisation to continue.</p>	
Name (Print): .....	Job Title:
Signature:	Date:
Renewal Time: From:	Date:

Date of first review:	
Date of subsequent reviews of this authorisation:	

**NB: A copy of this Form, once it has been authorised together with a copy of the original authorisation must be sent to the Corporate Director of Governance within 1 week of signing for placing on the Birmingham City Council's central register**

# BIRMINGHAM CITY COUNCIL

<b>STRICTLY PRIVATE &amp; CONFIDENTIAL</b>
--

## FORM B4: CANCELLATION OF AN AUTHORISATION FOR THE USE OR CONDUCT OF A COVERT HUMAN INTELLIGENCE SOURCE

### PART II OF THE REGULATION OF INVESTIGATORY POWERS ACT 2000 (RIPA)

**Guidance Note:**

1. After 1 April 2003, only Authorised Officers who have been certified by the Corporate Director of Governance will be allowed to sign RIPA Forms.
2. Applicants and Authorised Officers must comply, in full, with the Act and the City Council's Corporate Policy & Procedures Document and any other guidance issued, from time to time, by the Corporate Director of Governance. If in doubt, contact the Corporate Director of Governance, Mirza Ahmad, MBA, LL.M Barrister, Ingleby House, 11-14 Cannon Street, Birmingham B2 5EN. Tel: 0121 303 9991. Fax: 0121 303 1312. E-mail: mirza\_ahmad@birmingham.gov.uk
3. Copy of completed forms must be sent (once authorised or rejected) to the Corporate Director of Governance within 1 week of the authorisation, review, renewal, cancellation or rejection for the Central Register.
4. All boxes in this form must be completed. NOT APPLICABLE, N/A or lines must be put through irrelevant boxes.

**SECTION 1 (To be completed by the Applicant)**

<b>Subject of Surveillance:</b>		<b>Unique Reference Number (URN):</b>	/ /
			Year / Dept / Number

<b>Name of Applicant:</b>		<b>Unit/Division:</b>	
<b>Full Address:</b>			
<b>Contact Details:</b>			
<b>Investigation/ Operation Name: (if applicable)</b>			
<b>Form B1 URN:</b>		<b>From B2 URN:</b>	<b>From B3 URN:</b>

**Details of cancellation:**

<b>1. Explain the reason(s) for the cancellation of the authorisation:</b>

<b>2. Explain the value of the source in the operation:</b>

**SECTION 2 (To be completed by the Authorised Officer)**

<b>3. Authorised Officer's statement:</b>
I hereby authorise the cancellation of the use or conduct of the source as detailed above.
<b>Name (Print):</b> ..... <b>Grade:</b> .....
<b>Signature:</b> ..... <b>Date:</b> .....

<b>4. Time and Date of when the Authorised Officer instructed the use of the source to cease:</b>
<b>Date:</b> ..... <b>Time:</b> .....

<b>5. Authorisation cancelled:</b>	<b>Date:</b> .....	<b>Time:</b> .....
------------------------------------	--------------------	--------------------

**NB: A copy of this notice, once it has been authorised together with a copy of the authorisation (Form C3) must be sent to the Corporate Director of Governance within 1 week of the authorisation for placing on the Birmingham City Council's central register**

## **ACQUISITION OF COMMUNICATIONS DATA FORMS**

<b>Form ACD 1:</b>	Application form for Communications Data
<b>Form ACD 2</b>	Application for Communications Data SPOC Rejection Form
<b>Form ACD 3</b>	SPOC Log Sheet
<b>Form ACD 4</b>	SPOC Officer Report
<b>Form ACD 5</b>	Designated Person's Consideration Form
<b>Form ACD 6</b>	Authorisation Under Section 22(3) under the RIPA Act 2000
<b>Form ACD 7</b>	Notice under Section 22(4) under the RIPA Act 2000
<b>Form ACD 8</b>	Cancellation under Section 22(4)(8) under the RIPA Act 2000
<b>Form ACD 9</b>	Cancellation of Notice issued under Section 22(4)(8) of the RIPA Act 2000
<b>Form ACD 10</b>	Cancellation of Authorisation under Section 22(4)(8) of the RIPA Act 2000

**NB: If in doubt, ask the Corporate Director of Governance BEFORE any forms are used.**

# **Guidance Notes for the Submission of Communications Data Requests**

1. With the commencement of the new regulations under RIPA regulating the access to communications data, the old systems of simple application to the Communications Service Providers (CSP) under the varying pieces of legislation empowering officers to obtain information are defunct and must not be used.
2. All applications for communications data must now be through the Home Office approved Single Point of Contact Officer(s) (SPOC(s)) on the approved RIPA forms and be authorised by the Senior Assistant, Director Regulatory Services.

## **The New Regime.**

3. Part 1 Chapter II of the Regulation of Investigatory Powers Act 2000 (Acquisition and Disclosure of Communications Data) gives public authorities the power to acquire communications data. It came into force on the 5<sup>th</sup> January 2004.
4. Part I introduces a statutory framework to regulate access to communications data by public authorities consistent with the Human Rights Act 1998. It explains the duties and responsibilities placed upon each party involved in these processes, and creates a system of safeguards, reflecting the requirements of Article 8 of the ECHR.
5. The Government and the Courts are concerned to balance the rights of the individual against the needs of society as a whole to be protected from crime and other public safety risks. In order to achieve this, the regime around applying for communications data needed changing, hence the implementation of RIPA which basically does two things:-
  - (a) Places the arrangements with service providers on a statutory basis – i.e. gives public authorities lawful access to communications data
  - (b) Tightens the access to communications data considerably
6. There are certain safeguards that will apply to all public authorities that access communications data under RIPA. These provide further reassurance that the exercise of the powers under RIPA, take account of proportionality and necessity considerations and that scope for abuse is minimised. They are: -
  - Specifying clearly the persons designated to seek access to data;
  - An accreditation scheme for certain individuals with access to communications data;
  - Compliance with RIPA Code of Practice;
  - Oversight by the Interception Commissioner; and sanctions for the abuse of powers to access communications data under RIPA.

## 8. **What is Communications Data and what categories are there?**

RIPA defines communications data in three broad categories: -

### (a) **Section 21(4)(c) Information about communications service users**

This category mainly includes personal records supplied to the CSP by the customer/subscriber. For example, their name and address, payment method, contact number etc.

(b) **Section 21(4)(b) Information about the use of communications services**

This category mainly includes everyday data collected related to the customer's use of their communications system. For example, details of the dates and times they have made calls and which telephone numbers they have called.

(c) **Section 21(4)(a) Information about communications data (traffic data)**

This category mainly includes data generated by the CSP (network data) relating to a customer's use of their communications system (that the customer may not be aware of). for example, cell site data and routing information.

9. Not all public authorities have been given the power to access all three of these categories.  
**Local Government only has power to request data under Section 21(4) (b) & (c) not Section 21(4)(a)**

10. **What types of communications data are available?**

(a) **Section 21(4)(c) - Information about communications service users**

- Name of account holder/subscriber
- Installation and billing address (es)
- Method of payment/billing arrangements
- Collection/delivery arrangements for a PO Box (i.e. whether it is collected or delivered – not where it is collected from or delivered to)
- Other customer information such as any account notes, demographic information or sign up data (not passwords or personalised access information)

(b) **Section 21(4)(b) - Information about the use of communications services**

- Outgoing calls on a landline telephone or contract or prepay mobile phone
- Timing and duration of service usage
- Itemised connection records
- e-mail logs (sent)
- Information about the connection, disconnection and re-connection of services.
- Information about the provision of conference calling, call messaging, call waiting and call barring
- Information about the provision and use of forwarding/redirection services (postal and telecom)
- Records of postal items, such as records of registered, recorded or special delivery postal items, records of parcel consignment, delivery and collection.

(c) **Section 231(4)(a) Traffic data (not available to local authorities)**

- Information identifying the sender and recipient (including copy recipients) of a communication.
- Information identifying any location of a communication (such as mobile phone cell site location data)

- Routing information identifying or selecting any apparatus through which a communications is transmitted – for example dynamic IP address allocation, web postings and e-mail headers.
  - Call detail records for specific calls (such as calling line identity – incoming calls)
  - Web browsing information (only the web site name is disclosed and not the pages visited on that site)
- Information written on the outside of a postal item (such as a letter or a parcel)
- Online tracking of communications (including postal)
- Signalling information and dialling sequences that affects the routing of a communication (but not the delivery of information) in the investigation of “dial thru” fraud.

11. **What Purpose Can Communications Data Be Accessed?**

Under Section 22 (2) Local authorities can only access data for the: -

**PREVENTION AND DETECTION OF CRIME OR PREVENTING DISORDER**  
[Section 22(2)(b)]

12. **Applying for Communications Data.**

The procedure will be as follows: -

- (a) Each officer must complete the application form (ACD 1) in full, no sections should be omitted. (This form is subject to inspection by the Interception Commissioner and the applicant may be asked to justify their application)
- (b) Two forms of authorisation are possible: -
  - (i) An authorisation under Section 22(3) of the Act. This authorises the applicant to personally extract the data from the CSP's records. (This will rarely be used by TS as its intended use is where there may be a security breach at the CSP and asking the CSP to provide the data would forewarn or alert the subject)
  - (ii) A notice under section 22(4) requiring the CSP to extract the communications data specified from its records and to send that data to the SPOC (normal request).

The applicant must indicate which authorisation he seeks.

- (c) The form is then submitted to the SPOC (John Martin or in his absence Huw Jones).
- (d) The SPOC will then assess whether the form is completed properly, that it is a request which is lawful and to which the CSP can practically respond, that the cost and resource implications for the CSP / authority are within reason.
- (e) The SPOC will then submit the form to the designated person for authorisation (Snr. Asst. Director Regulatory Services) (This form as previously stated is subject to inspection by the Interception Commissioner and therefore the designated person maybe called upon to justify any decisions made).

- (f) If the application is rejected either by the SPOC or the designated person the SPOC will retain the form and inform the applicant in writing of the reasons for its rejection (ACD 2)
  - (g) Once authorised the SPOC will forward the application to the CSP.
  - (h) Once the data sought is returned to the SPOC a copy of the information will be passed to the applicant.
  - (i) All original documents will be retained by the SPOC (copies will be sent to the Corporate Director of Governance of the city council, who acts as the monitoring officer for the authority) until the Interception Commissioner has inspected the authority and given permission for the records to be destroyed.
  - (j) There are a number of other administrative forms that the SPOC's are obliged to complete as the application is progressed, although these will not necessarily involve operational officer.
13. If you are at all unsure about anything to do with these ACD forms, please contact John Martin, Huw Jones or Mirza Ahmad for advice **before** using any of the forms.

# ACD FLOWCHART

This procedure is mandatory under Regulation of Investigatory Powers Act 2000 (RIPA)

Guidance Notes for the Submission of Communication Data Requests – **Appendix 5** -details the background to and application of RIPA to communication requests

Officer requesting communication data must satisfy themselves that it falls within the scope of section 24 (1) (b) or (c) – See **ACD1**

Requesting Officer completes application form – **ACD2** –in full, no sections to be omitted (inc CSP)

Form passed to Line Manager to confirm, by signature, the facts contained in the request

Request Form passed electronically to SPOC  
(J Martin [H.Jones] in his absence)

SPOC assesses if form completed correctly, that request is lawful and to which the Communications Service Providers (CSP) can practically respond, that cost and resource implications for the Authority are within reason

If SPOC rejects request **ACD3** rejection form sent to Officer

SPOC submits form to Senior Assistant Director Regulatory Services for authorisation

If SAD rejects request, SPOC sends **ACD3** rejection form to Officer

SPOC forwards application to CSP  
**ACD 4 -10** may apply

Copy of information received from CSP resulting from the application forwarded to Officer by SPOC

SPOC retains all original documents until the Interception Commissioner has inspected the Authority

# BIRMINGHAM CITY COUNCIL

**STRICTLY PRIVATE  
& CONFIDENTIAL**

## **FORM C1: APPLICATION FOR AUTHORISATION TO CARRY OUT DIRECTED SURVEILLANCE IN RELATION TO EMPLOYEES**

**THIS IS NOT A RIPA AUTHORISATION FORM.  
THIS FORM SHOULD NOT BE USED FOR  
AUTHORISING RIPA SURVEILLANCE**

**Guidance Note:**

1. After 1 April 2003, only Authorising Officers who have been certified by the Corporate Director of Governance will be allowed to authorise Surveillance Forms.
2. Applicants and Authorising Officers must comply, in full, with the Act and the City Council's Corporate Policy & Procedures Document and any other guidance issued, from time to time, by the Corporate Director of Governance. If in doubt, contact the Corporate Director of Governance, Mirza Ahmad, MBA, LL.M Barrister, Ingleby House, 11-14 Cannon Street, Birmingham B2 5EN. Tel: 0121 303 9991. Fax: 0121 303 1312. E-mail: mirza\_ahmad@birmingham.gov.uk
3. All boxes in this form must be completed. NOT APPLICABLE, N/A or lines must be put through irrelevant boxes.

**Subject of Surveillance**

*(including full address)*

### **SECTION 1 (to be completed by the Applicant)**

**Name of Applicant**

**Unit/Division**

**Full Address**

**Contact Details**

**Investigation/Operation  
Name (if applicable)**

**Details of application:**

**3. Give name / job title of Authorised Officer:**

**4. Describe the purpose of the specific investigation or operation.**

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

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

- Name:
- Address:
- DOB:
- Other known / relevant information:

**5. Explain the information that is desired to obtain as a result of the directed surveillance:**

**6. Explain why directed surveillance is NECESSARY in this particular case:**

**7. Supply details of any potential COLLATERAL INTRUSION and why the intrusion is unavoidable:  
(Also describe precautions to MINIMISE collateral intrusion)**

**8. Explain why the directed surveillance is PROPORTIONATE to what it seeks to achieve. How intrusive might it be or the subject of surveillance or on others? And why is this intrusion outweighed by the need for surveillance in operational terms or can the evidence be obtained by any other means?**

**9. Confidential information (e.g. confidential legal privilege, personal information and journalistic material)**

INDICATE THE LIKELIHOOD OF ACQUIRING ANY CONFIDENTIAL INFORMATION

**10. Applicant's Details.**

Name (print)

Tel No:

Job Title

Date

Signature

**11. Anticipated Start Date Time**

Date:

Time:

**SECTION 2 (To be completed by the Authorised Officer)**

**12. Authorised Officer's Statement must spell out the "5 W's" – Who; What; Where; Why and How.**

**1. I hereby authorise as follows:**

*Who is authorised to conduct surveillance:*

*What is authorised for the surveillance:*

*Where is it to take place and for how long:*

*Why is it being authorised:*

*How will the surveillance be conducted:*

2. This written authorisation will cease to have effect at the end of a period of 3 months unless renewed (see separate form for renewals).
3. The Applicant and the Authorised Officer will jointly review this authorisation on the date below to see whether the authorisation should continue, be renewed or cancelled.

**13. Authorised Officer's statement explaining why in his / her view the directed surveillance is necessary and proportionate. This box must be completed and both aspects must be addressed.**

Why is it necessary?

Why is it proportionate?

**14. Confidential Information Authorisation. Supply details demonstrating compliance with Home Office Codes of Practice relating to this issue.**

**Expiry of Authorisation (3 months from date / time of Authorisation unless stated here):**

**Date of first review:**

**Date of subsequent reviews of this Authorisation:**

**Authorised Officer's Name:**

**Job Title:**

**Signature:**

**Date / Time:**

**16. Urgent Authorisation: Authorised Officer to explain why s/he considered the case so urgent that an oral, instead of a written, authorisation was given.**

**URGENT AUTHORISATION EXPIRY DATE / TIME :  
(72 HOURS) AFTER ORAL AUTHORISATION).**

**A copy of this Form, once it has been authorised or refused, must be held on the investigating officer's file.**

**There is no requirement to place a copy of the authorisation on the Corporate Database**

# BIRMINGHAM CITY COUNCIL

**STRICTLY PRIVATE  
& CONFIDENTIAL**

## FORM C2: REVIEW OF A DIRECTED SURVEILLANCE AUTHORISATION IN RELATION TO EMPLOYEES

**THIS IS NOT A RIPA AUTHORISATION FORM.  
THIS FORM SHOULD NOT BE USED FOR  
AUTHORISING RIPA SURVEILLANCE**

**Guidance Note:**

1. After 1 April 2003, only Authorising Officers who have been certified by the Corporate Director of Governance will be allowed to authorise surveillance.
2. Applicants and Authorising Officers must comply, in full, with the Act and the City Council's Corporate Policy & Procedures Document and any other guidance issued, from time to time, by the Corporate Director of Governance. If in doubt, contact the Corporate Director of Governance, Mirza Ahmad, MBA, LL.M Barrister, Ingleby House, 11-14 Cannon Street, Birmingham B2 5EN. Tel: 0121 303 9991. Fax: 0121 303 1312. E-mail: mirza\_ahmad@birmingham.gov.uk
3. All boxes in this form must be completed. NOT APPLICABLE, N/A or lines must be put through irrelevant boxes.

### SECTION 1 (To be completed by the Applicant)

<b>Subject of Surveillance:</b>	
---------------------------------	--

<b>Name of Applicant:</b>		<b>Unit/Division:</b>			
<b>Full Address:</b>					
<b>Contact Details:</b>					
<b>Operation Name:</b>		<b>Form A1 URN</b>	(Dept)	(Year)	(Number)
<b>Date of authorisation or last renewal:</b>		<b>Expiry date of authorisation or last renewal:</b>			
		<b>Form A2 URN</b>			

**Details of review:**

<b>1. Review number and dates of any current and previous reviews:</b>	
<b>Review Number:</b>	<b>Date:</b>

<b>2. Summary of the investigation/operation to date, including what private information has been obtained and the value of the information so far obtained:</b>

<b>3. Detail the reasons why it is NECESSARY to continue with the directed surveillance:</b>

<b>4. Explain how the proposed activity is still PROPORTIONATE to what it seeks to achieve:</b>

<b>5. Detail any incidents of collateral intrusion and the likelihood of any further incidents of collateral intrusions occurring:</b>

**6. Give details of any confidential information acquired or accessed and the likelihood of acquiring confidential information:**

--

**7. Applicant's Details:**

**Name (Print):**

**Tel No:**

**Job Title:**

**Date:**

**Signature:**

**SECTION 2 (To be completed by the Authorised Officer)**

**8. Authorised Officer's Comments, including whether or not the directed surveillance should continue:**

--

**9. Authorised Officer's Statement:**

I hereby agree that the directed surveillance, as detailed above, should [continue until its next review] [be cancelled immediately].

**Name (Print):**

.....

**Job Title:**

**Signature:**

**Date:**

**11. Date of next review:**

--

**A copy of this Form, once it has been authorised or refused, must be held on the investigating officer's file.**

**There is no requirement to place a copy of the authorisation on the Corporate Database**

# BIRMINGHAM CITY COUNCIL

**STRICTLY PRIVATE  
& CONFIDENTIAL**

## **FORM C3: APPLICATION FOR RENEWAL OF A DIRECTED SURVEILLANCE AUTHORISATION IN RELATION TO AN EMPLOYEE**

**(Please attach a copy of the original authorisation)**

**THIS IS NOT A RIPA AUTHORISATION FORM.  
THIS FORM SHOULD NOT BE USED FOR  
AUTHORISING RIPA SURVEILLANCE**

**Guidance Note:**

1. After 1 April 2003, only Authorising Officers who have been certified by the Corporate Director of Governance will be allowed to authorise surveillance.
2. Applicants and Authorising Officers must comply, in full, with the Act and the City Council's Corporate Policy & Procedures Document and any other guidance issued, from time to time, by the Corporate Director of Governance. If in doubt, contact the Corporate Director of Governance, Mirza Ahmad, MBA, LL.M Barrister, Ingleby House, 11-14 Cannon Street, Birmingham B2 5EN. Tel: 0121 303 9991. Fax: 0121 303 1312. E-mail: mirza\_ahmad@birmingham.gov.uk
3. All boxes in this form must be completed. NOT APPLICABLE, N/A or lines must be put through irrelevant boxes.

**SECTION 1 (To be completed by the Applicant)**

<b>Subject of Surveillance:</b>			
<b>Name of Applicant:</b>		<b>Unit/ Division:</b>	
<b>Full Address:</b>			
<b>Contact Details:</b>			
<b>Investigation/ Operation Name: (if applicable)</b>			
<b>Renewal Number</b>			

**Details of renewal:**

<b>12. Renewal numbers and dates of any current and previous renewals:</b>	
<b>Renewal Number</b>	<b>Date:</b>

<b>13. Detail any significant changes to the information provided in the original authorisation, as it applies at the time of the renewal:</b>

<b>14. Detail the reasons why it is NECESSARY to continue with the directed surveillance:</b>

<b>15. Detail why the directed surveillance is still PROPORTIONATE to what it seeks to achieve:</b>

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

**17. Give details of the results of the regular reviews of the investigation or operation:**

**18. Applicant's Details:**

**Name (Print):**

**Tel No:**

**Job Title:**

**Date:**

**Signature:**

**SECTION 2 (To be completed by the Authorised Officer)**

**19. Authorised Officer's Comments: This box must be completed to indicate why the renewal (if agreed) is necessary and proportionate.**

**20. Authorised Officer's Statement:**

I hereby authorise [or reject] the renewal of the directed surveillance operation as detailed above. The renewal (if authorised) will last for 3 months unless renewed in writing.

This renewal will be reviewed frequently to assess the need for the authorisation to continue.

**Name (Print):** ..... **Job Title:**

**Signature:** ..... **Date:**

**Renewal Time:** ..... **Date:**  
**From:**

<b>Date of first review:</b>	
<b>Date of subsequent reviews of this authorisation:</b>	

**A copy of this Form, once it has been authorised or refused, must be held on the investigating officer's file.**

**There is no requirement to place a copy of the authorisation on the Corporate Database**

# BIRMINGHAM CITY COUNCIL

**STRICTLY PRIVATE  
& CONFIDENTIAL**

## **FORM C4: CANCELLATION OF A DIRECTED SURVEILLANCE AUTHORISATION IN RELATION TO AN EMPLOYEE**

**THIS IS NOT A RIPA AUTHORISATION FORM.  
THIS FORM SHOULD NOT BE USED FOR  
AUTHORISING RIPA SURVEILLANCE**

**Guidance Note:**

1. After 1 April 2003, only Authorising Officers who have been certified by the Corporate Director of Governance will be allowed to authorise surveillance.
2. Applicants and Authorising Officers must comply, in full, with the Act and the City Council's Corporate Policy & Procedures Document and any other guidance issued, from time to time, by the Corporate Director of Governance. If in doubt, contact the Corporate Director of Governance, Mirza Ahmad, MBA, LL.M Barrister, Ingleby House, 11-14 Cannon Street, Birmingham B2 5EN. Tel: 0121 303 9991. Fax: 0121 303 1312. E-mail: mirza\_ahmad@birmingham.gov.uk
3. All boxes in this form must be completed. NOT APPLICABLE, N/A or lines must be put through irrelevant boxes.

**SECTION 1 (To be completed by the Applicant)**

<b>Subject of Surveillance:</b>			
<b>Name of Applicant:</b>		<b>Unit/Division:</b>	
<b>Full Address:</b>			
<b>Contact Details:</b>			
<b>Investigation /Operation Name: (if applicable)</b>			

**Details of cancellation:**

<b>5. Explain the reason(s) for the cancellation of the authorisation:</b>

<b>6. Explain the value of surveillance in the operation:</b>

**SECTION 2 (To be completed by the Authorised Officer)**

<b>7. Authorised Officer's statement:</b>
I hereby authorise the cancellation of the directed surveillance as detailed above.
<b>Name (Print):</b> .....
<b>Job Title:</b> .....
<b>Signature:</b> .....
<b>Date:</b> .....

<b>8. Time and Date of when the Authorised Officer instructed the surveillance to cease:</b>
<b>Date:</b> .....
<b>Time:</b> .....

<b>5. Authorisation cancelled:</b> .....
<b>Date:</b> .....
<b>Time:</b> .....

**A copy of this Form, once it has been authorised or refused, must be held on the investigating officer's file.**

**There is no requirement to place a copy of the authorisation on the Corporate Database**