



# CHELTENHAM BOROUGH COUNCIL

**CHELTENHAM BOROUGH COUNCIL**

**REGULATION OF INVESTIGATORY POWERS ACT 2000**

**PROCEDURAL GUIDE**

**October 2010**

**Document History****Document Location** T:\Policy and partnerships\Policy folders\RIPA (protected file)**Control location** Code of Corporate Governance Appendix A**Review Period** Annual**Reviewed by** Corporate Governance Group and Economy and Business Improvement Overview & Scrutiny Committee

<b>Version Number</b>	<b>Version Date</b>	<b>Summary of Changes</b>
<b>1.0</b>	<b>14/02/2007</b>	<b>New Guidance</b>
<b>1.1</b>	<b>27/04/2010</b>	<b>Legislative and administrative changes</b>
<b>1.2</b>	<b>09/08/2010</b>	<b>Comments from EB&amp;I</b>
<b>1.3</b>	<b>26/10/2010</b>	<b>Cabinet approval</b>

**This document is owned by:**

<b>Name</b>	<b>Job Title</b>	<b>Version</b>
Jane Griffiths	Assistant Chief Executive	1.1
Jane Griffiths	Assistant Chief Executive	1.2
Jane Griffiths	Assistant Chief Executive	1.3

**This document has been distributed to**

<b>Name</b>	<b>Job Title</b>	<b>Version</b>
All CBC staff Public website		1.0
All CBC staff Public website Cabinet		1.1 June 2010
EB&I overview and scrutiny		1.2 20/09/2010
Cabinet Intranet and internet		1.3

The Government is currently reviewing the Regulation of Investigatory Powers Act 2000 and this guidance will need to be reviewed further to reflect those changes.

## **Forward**

The purpose of this Procedural Guide ("the Guide") is to ensure that Cheltenham Borough Council ("the Council") complies with the Regulation of Investigatory Powers Act 2000 (RIPA).

The Act and this guidance make provision for and about the interception of communications, the acquisition and disclosure of data relating to communications, the carrying out of surveillance, the use of covert human intelligence sources and the acquisition of the means by which electronic data protected by encryption or passwords may be decrypted or accessed; to provide for Commissioners and a tribunal with functions and jurisdiction in relation to those matters, to entries on and interferences with property or with wireless telegraphy and to the carrying out of their functions by the Security Service, the Secret Intelligence Service and the Government Communications Headquarters; and for connected purposes.

The introduction of the Human Rights Act 1998 means that the Council by law has to respect the rights of everyone. In particular Article 8 guarantees everyone the right to respect for their private and family life, their home and correspondence. This right can only be interfered with when the interference is in accordance with the law and necessary. RIPA provides the framework for public authorities to carry out surveillance and the lawful means whereby rights can be infringed by the Council. If the correct procedures are put in place and followed by officers the Council will earn the protection of RIPA and our actions will be lawful.

Cheltenham Borough Council undertakes to use these powers in line with the law, sparingly and proportionately.

Steve Jordan  
Leader  
Cheltenham Borough Council

## Index

Section	Section number
Introduction	1
The background to RIPA	2
The scope of this guide	2.2
Consequences of not following RIPA	2.3
The Surveillance Commissioner	2.4
Covert Surveillance	3
Directed Surveillance (DS)	3.1
Covert Human Intelligence Sources (CHIS)	3.2
Intrusive surveillance	3.3
Procedure for obtaining authorisations	4.0
The Senior Responsible Officer;-	4.1
Authorising Officers	4.3
Investigating Officers – What you need to do before applying for authorisation	4.4
Duration, review, renewal and cancellation of authorisations	5.0
Duration	5.1
Review	5.2
Renewals	5.3
Cancellations	5.4
The RIPA Coordinator	6.0
Legal Advice	7.0
Officers	Appendix A
Authorisation Forms	Appendix B
Flow chart Will _ DCS authorisation be required	Appendix C

## 1 INTRODUCTION

- 1.1 This policy document shall be readily available at the offices of Cheltenham Borough Council (“the Council”). A copy can be obtained from the RIPA co-ordinator, Policy and Partnerships, Municipal Offices, Promenade, Cheltenham, GL50 9SA.  
It is also available on the Council's website at [www.cheltenham.gov.uk](http://www.cheltenham.gov.uk) and the Intranet.
- 1.2 The purpose of this document is to ensure that the Council complies with the Regulation of Investigatory Powers Act 2000 (RIPA).
- 1.3 This document provides guidance on the regulation of any covert surveillance that is carried out by council officers. This includes the use of undercover officers, informants and private investigators and other agents of the Council.
- 1.4 Any covert surveillance will have to be authorised and conducted in accordance with RIPA, the statutory codes of practice and this Guide and shall only be for one of the purposes set out in this Guide and for a purpose which the Council is legally required or empowered to investigate as part of its functions.
- 1.5 Covert surveillance will only be used by the Council where it judges such use to be proportionate to the seriousness of the crime or matter being investigated, and the history and character of the individual(s) concerned.
- 1.6 Before requesting authorisation Investigating Officers will have regard to this document and the statutory Codes of Practice issued under section 71 RIPA. The Codes of Practice are available from the RIPA co-ordinator and direct from the Office of Surveillance website at <http://www.surveillancecommissioners.gov.uk/> or the Home Office at <http://security.homeoffice.gov.uk/ripa/>.
- 1.7 Before authorising covert surveillance Authorising Officers will have regard to this Guide and the statutory Codes of Practice issued under section 71 RIPA. The Codes of Practice are available from the RIPA co-ordinator and direct from the Office of Surveillance website at <http://www.surveillancecommissioners.gov.uk/> or the Home Office at <http://security.homeoffice.gov.uk/ripa/>.
- 1.8 Authorising officers will have to consider whether it is necessary and proportionate for Investigating Officers to undertake covert surveillance and whether it is possible to obtain the evidence through other means.
- 1.9 Authorising Officers must give detailed consideration to the risk of collateral intrusion i.e. the risk of intruding into the privacy of others while watching someone else. This consideration will need to be recorded within the RIPA file.
- 1.10 There must be no situation where an officer engages in covert surveillance without obtaining authorisation in accordance with the procedures set out in this document, the statutory Codes of Practice and from RIPA.
- 1.11 Any queries concerning the content of the document should be addressed to the RIPA co-ordinator.

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

### **2.1 The background to RIPA**

RIPA provides a legal framework for the control and regulation of surveillance and information techniques which public authorities undertake as part of their duties. As was highlighted in the introduction to the Guide the need for such control arose as a result of the Human Rights Act 1998. Article 8 of the European Convention on Human Rights states that: -

- 1) *Everyone has the right of respect for his private and family life, his home and his correspondence.*
- 2) *There shall be no interference by a public authority with the exercise of this right except such as in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health and morals or for the protection of the rights and freedoms of others.*

The right under Article 8 is a qualified right and authorities can interfere with this right for the reasons given in paragraph 2 of Article 8. RIPA provides the legal framework for lawful interference.

### **2.2 The scope of this Guide**

This Guide intends to cover the surveillance and information gathering techniques which are most likely to be carried out by the Council.

Neither RIPA nor this Guide covers the use of any overt surveillance, general observation that forms part of the normal day to day duties of officers, the use of equipment to merely reinforce normal sensory perception such as binoculars or circumstances where members of the public who volunteer information to the Council.

RIPA does not normally cover the use of overt CCTV surveillance systems since members of the public are aware that such systems are in place.

There may however be times when the Council uses the CCTV for a specific investigation or operation. This Guide does not cover in detail the use of surveillance via the Town Centre CCTV system. In such cases authorisation for directed surveillance may be required. If the CCTV is to be used for surveillance, Investigating Officers should consult and adhere to the provisions of the Cheltenham Town Centre Closed Circuit Television Operating Procedures and the Cheltenham Town Centre Closed Circuit Television Codes of Practice jointly set up by Cheltenham Borough Council and Gloucestershire Constabulary.

If an Investigating Officer envisages using any other CCTV system they should contact the RIPA co-ordinator concerning any clarification on the administrative process or seek legal advice from OneLegal before they conduct any surveillance.

RIPA deals with a wide variety of surveillance types. Some of the other techniques that are covered by RIPA but will not or cannot be used by local authorities are listed below, these include: -

1. The interception of any communication such as postal, telephone or electronic communications without both the sender and receiver's permission;
2. The acquisition and disclosure of information to who has sent or received any postal, telephone or electronic communication; and
3. The covert use of surveillance equipment within any premises or vehicle, including business premises and vehicles with the intention of covertly gathering information about the occupant/s of such premises or vehicles

The interference of telecommunications sent and received by Council staff is considered in chapter 7.

### **2.3 Consequences of not following RIPA**

Section 27 of RIPA provides that surveillance shall be lawful for all purposes if authorised and conducted in accordance with an authorisation granted under RIPA.

Lawful surveillance is exempted from civil liability.

Although not obtaining authorisation does not make the authorisation unlawful per se, it does have some consequences: -

- i. Evidence that is gathered may be inadmissible in court;
- ii. The subjects of surveillance can bring their own proceedings or defeat proceedings brought by the Council against them on human rights grounds i.e. we have infringed their rights under Article 8;
- iii. If a challenge under Article 8 is successful the Council could face a claim for financial compensation;
- iv. A complaint could be made to the Office of Surveillance Commissioners; and
- v. The government has also introduced a system of tribunal. Any person who believes that their rights have been breached can have their complaint dealt with by way of a tribunal.

### **2.4 The Surveillance Commissioner**

The government has appointed a Surveillance Commissioner to review the way in which public authorities implement the requirements of RIPA. The Commissioner has a wide range of powers of access and investigation. The Council will receive periodic visits from the Office of the Surveillance Commissioners. They will check to see if the Council is complying with RIPA.

It is important that we can show that we all comply with this Guide and comply with the provisions of RIPA.

## **3 COVERT SURVEILLANCE**

There are three categories of covert surveillance: -

1. Directed Surveillance;
2. Covert Human Intelligence Sources; and
3. Intrusive surveillance (but nothing in this Procedure permits the authorising of "Intrusive Surveillance" as defined in RIPA (i.e. in respect of anything taking place on residential premises or in a private vehicle, involving the presence of an investigator on those premises/vehicles or carried out through a surveillance device)).

### **3.1 Directed Surveillance (DS)**

The majority of covert surveillance that will be undertaken by the Council will fall under the heading of Directed Surveillance (DS).

DS is defined as surveillance which is covert, but not intrusive, and is undertaken:

- a) For the purpose of a specific investigation or operation
- b) In such a manner as it is likely to result in obtaining private information about a person (whether or not that person is the target of the investigation or operation) and
- c) In a planned manner and not by way of an immediate response whereby it would not be reasonably practicable to obtain an authorisation prior to the surveillance being carried out.

It is irrelevant where the subject of the DS is being observed.

If you intend to instruct an agent to carry out the DS the agent must complete and sign the form marked "agent's agreement form" contained in Appendix C. The agent will be subject to RIPA in the same way as any employee of the Council would be.

The flow chart in Appendix D gives guidance on when authorisation might be needed.

### **3.2 Covert Human Intelligence Sources (CHIS)**

This involves the establishment or maintenance of a personal or other relationship with a person for the covert purpose of obtaining or disclosing private information. A CHIS is a person who: -

- a) s/he establishes or maintains a personal or other relationship with a person for the covert purpose of facilitating the doing of anything falling within paragraph b) or c);
- b) he covertly uses such a relationship to obtain information or to provide access to any information to another person; or
- c) he covertly discloses information obtained by the use of such a relationship or as a consequence of the existence of such a relationship.



- 3.2.1 A relationship is established or maintained for a covert purpose if and only if it is conducted in a manner that is calculated to ensure that one of the parties to the relationship is unaware of the purpose.
- 3.2.2 A relationship is used covertly, and information obtained is disclosed covertly, if and only if the relationship is used or the information is disclosed in a manner that is calculated to ensure that one of the parties to the relationship is unaware of the use or disclosure in question.
- 3.2.3 Covert human intelligence sources may only be authorised if the following arrangements are in place:
- that there will at all times be an officer within the local authority who will have day to day responsibility for dealing with the source on behalf of the authority, and for the source's security and welfare;
  - that there will at all times be another officer within the local authority who will have general oversight of the use made of the source;
  - that there will at all times be an officer within the local authority who has responsibility for maintaining a record of the use made of the source; and
  - that the records relating to the source maintained by the local authority will always contain particulars of all matters specified by the Secretary of State in Regulations.
- 3.2.4 Legal advice should always be sought where any matters for investigation may involve the use of other enforcement agencies, including the police.
- 3.2.5 Special consideration must be given to the use of vulnerable individuals for CHIS. 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 unable to protect himself against significant harm or exploitation. Any individual of this description, or a juvenile as defined below, should only be authorised to act as a source in the most exceptional circumstances and only then when authorised by the Chief Executive (or, in his absence, the Deputy Chief Executive).
- 3.2.6 Before you undertake any surveillance involving a vulnerable individual you **must obtain legal advice and** consult the RIPA co-ordinator concerning any clarification on the administrative process. Also in these cases, an Assistant Director must agree to the use of a vulnerable individual before authorisation is sought from the Chief Executive officer
- 3.2.7 Special safeguards also apply to the use or conduct of juvenile sources; that is sources under the age of 18 years. On no occasion should the use or conduct of a source under 16 years of age be authorised to give information against his parents or any person who has parental responsibility for him.

- 3.2.8 In other cases, authorisations should not be granted unless the special provisions contained within The Regulation of Investigatory Powers (Juveniles) Order 2000; SI No. 2793 are satisfied. Authorisations for juvenile sources should be granted by Chief Officers. Before you undertake any surveillance involving a juvenile you **must** consult the RIPA co-ordinator concerning any clarification on the administrative process or seek legal advice from OneLegal.
- 3.2.9 If you intend to instruct an agent to carry out the CHIS the agent must complete and sign the form marked "agent's agreement form" contained in Appendix C. The agent will be subject to RIPA in the same way as any employee of the Council would be.
- 3.2.10 The flow chart in Appendix D gives guidance on when authorisation might be needed.

### **3.3 Intrusive surveillance**

Intrusive surveillance is defined as covert surveillance that: -

- a) is carried out in relation to anything taking place on any residential premises or in any private vehicle; and
- b) involves the presence of any individual on the premises or in the vehicle or is carried out by means of a surveillance device.
- c) If the device is not located on the premises or in the vehicle, it is not intrusive surveillance unless the device consistently provides information of the same quality and detail as might be expected to be obtained from a device actually present on the premises or in the vehicle.

#### **3.3.1 LOCAL AUTHORITIES ARE NOT AUTHORISED TO CONDUCT INTRUSIVE SURVEILLANCE**

- 3.3.2 If you are considering conducting surveillance and the surveillance might fall within the scope of intrusive surveillance you **must** contact the RIPA co-ordinator concerning any clarification on the administrative process or seek legal advice from OneLegal before you undertake any surveillance.

## **4 PROCEDURE FOR OBTAINING AUTHORISATIONS**

### **4.1 The Senior Responsible Officer ;-**

Role:

4.1.1 The Chief Executive Officer is the Senior Responsible Officer is designated the Council's SRO with responsibilities for:

4.1.2 (a) ensuring the integrity of the Council's RIPA processes;

(b) ensuring compliance with RIPA legislation and the Home Office Codes of Practice;

(c) engaging with the OSC when its inspector conducts an inspection;

(d) overseeing the implementation of any post - inspection plans;

(e) ensuring that all Authorising Officers are of an appropriate standard in light of any recommendations made by the OSC inspection reports;

(f) ensuring that concerns are addressed, where OSC inspection reports highlight concerns about the standards of Authorising Officers.

### **4.2 Authorising Officers**

Role:

Authorising officers can authorise, review and cancel directed surveillance, and can authorise, review and cancel the employment of a juvenile or vulnerable CHIS, or the acquisition of confidential information

4.2.1 The Regulation of Investigatory Powers (Directed Surveillance and Covert Human Intelligence Sources) Order 2010 prescribes that for local authorities the Authorising Officer shall be a Director, Head of Service, Service Manager or equivalent as distinct from the officer responsible for the conduct of an investigation.

4.2.2 Officers of a lower rank **can not** grant authorisations even in cases of urgency.

4.2.3 A designated Authorising Officer must qualify **both** by rank and by competence. Officers who wish to be designated must have been trained to an appropriate level so as to have an understanding of the Act and the requirements that must be satisfied before an authorisation can be granted.

Appendix A lists the officers within the Council who can grant authorisations all of which are at Strategic or Assistant Director level.

- 4.2.4 Authorisations must be given in writing by the Authorising Officer. However In urgent cases authorisation may be given orally (by the Authorising Officer) who must then make a written record of the decision and reasons for it as soon as is reasonably practicable. Mere administrative convenience does not justify use of the urgent procedure.

A case is not normally to be regarded as urgent unless the time that would elapse before the authorising officer was available to grant the authorisation would, in the judgement of the person giving the authorisation, be likely to endanger life or jeopardise the investigation or operation for which the authorisation was being given. An authorisation is not to be regarded as urgent where the need for an authorisation has been neglected or the urgency is of the authorising officer's or applicant's own making

- 4.2.5 Authorising Officers are also responsible for carrying out regular reviews of applications which they have authorised and also for the cancellation of authorisations.

### **4.3 Investigating Officers – What you need to do before applying for authorisation**

- 4.3.1 Investigating Officers should think about the need to undertake DS or CHIS before they seek authorisation. Investigating Officers need to consider whether they can obtain the information by using techniques other than covert surveillance. There is nothing that prevents an Investigating Officer discussing the issue of surveillance beforehand. Any comments by a supervisor should be entered into the application for authorisation.

- 4.3.2 The Codes of Practice do however advise that Authorising Officers should not be directly responsible for authorising investigations or operations in which they are directly involved although it is recognised that this may sometimes be unavoidable.

- 4.3.3 If you intend to carry out DS or use CHIS you should complete and submit an Application for Directed Surveillance form which is marked "authds" in Appendix B or an Application for the use of CHIS to an Authorising Officer which is marked "authchis" in Appendix B.

- 4.3.4 Appendix D shows the steps which are required as part of the authorisation process.

- 4.3.5 The person seeking the authorisation should complete parts 1 and 2 of the form having regard to the guidance given in this Guide and the statutory Codes of Practice. If the situation is urgent, verbal authorisation should be obtained from the appropriate Authorising Officer. Urgent oral authorisation will cease to have effect after 72 hours unless cancelled or renewed (or replaced by the standard application for authorisation). As soon as it is reasonably practicable after the verbal authorisation has been given the authorisation form should be completed, including section 16 which deals with why the situation was considered urgent. The Codes of Practice offer guidance on when an application should be considered urgent.

- 4.3.6 The form should then be submitted to the Authorising Officer for authorisation.

### **4.4 Authorising Officers – What you need to do before authorising surveillance**

4.4.1 Before giving authorisation an Authorising Officer **must** be satisfied that the reason for the request is one of the permitted reasons under the Act and permitted under the Regulation of Investigatory Powers (Directed Surveillance and Covert Human Intelligence Sources) Order 2003 i.e.

- For the purpose of the prevention and detection of crime or for the preventing of disorder; and
- the desired result of the covert surveillance cannot reasonably be achieved by other means
- the risks of collateral intrusion have been properly considered, whether the reason for the surveillance is balanced proportionately against the risk of collateral intrusion
- there must also be consideration given to the possibility of collecting confidential personal information. If there is a possibility of collecting personal information the matter should be passed to the Chief Officer for consideration

- 4.4.2 An Authorising Officer **must** also be satisfied the surveillance in each case is **necessary and proportionate**.

This is defined as:

#### **Necessity**

- Obtaining an authorisation under the 2000 Act, the 1997 Act and 1994 Act will only ensure that there is a justifiable interference with an individual's Article 8 rights if it is necessary and proportionate for these activities to take place. The 2000 Act first requires that the person granting an authorisation believe that the authorisation is necessary in the circumstances of the particular case for one or more of the statutory grounds in section 28(3) of the 2000 Act for directed surveillance and in section 32(3) of the 2000 Act for intrusive surveillance.

#### **Proportionality**

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

When the Authorising Officer has considered if the surveillance is necessary and proportionate they must complete the relevant section of the form explaining why in his/her opinion the surveillance is necessary and proportionate. Any member of staff considering the use of RIPA for activities associated with fly tipping or dog fouling must request Onelegal to determine if the rules on necessity and proportionality have been met and their determination must be documented and submitted to the Authorising officer with the relevant form.

## **5 DURATION, REVIEW, RENEWAL AND CANCELLATION OF AUTHORISATIONS**

### **5.1 Duration**

- 5.1.1 2.1 DS authorisations will cease to have effect after three months from the date of approval unless renewed or cancelled.
- 2.2 Authorisations should be given for the maximum duration but reviewed on a regular basis and formally cancelled when no longer needed.
- 5.1.2 CHIS authorisations will cease to have effect after twelve months from the date of approval.
- 5.1.3 Investigating Officers should indicate within the application the period of time that they estimate is required to carry the surveillance, this will be proportionate to the objectives of the investigation and give due consideration to collateral intrusion

- 5.1.4 Urgent verbal authorisations will only be effective for up to 72 hours, from the time that the authorisation was granted, unless the authorisation is subsequently endorsed by a written authorisation.
- 5.1.5 For CHIS authorisations, legal advice must be sought, particularly those that involve the use of juveniles (for which the duration of such an authorisation is one month instead of twelve months).
- 5.1.6 It is the responsibility of the Investigating Officer to make sure that the authorisation is still valid when they undertake surveillance.

## **5.2 Review**

- 5.2.1 An Investigating Officer must carry out a regular review of authorisations. If an authorisation is no longer required or considered to be no longer *Necessary* or *Proportionate* it **must** be cancelled.
- 5.2.2 The results of any review must be included on the review form (see forms "revds" and "revchis" in Appendix B).
- 5.2.3 The Authorising Officer also has a duty to review authorisations that have been granted when it is necessary or practicable to do so. Particular attention should be given to authorisations involving collateral intrusion or confidential material.
- 5.2.4 The Authorising Officer should keep a copy of the review form and a copy should be given to the Investigating Officer. A copy of the review form must also be sent to the RIPA co-ordinator.

## **5.3 Renewals**

- 5.3.1 An Investigating Officer can ask for and an Authorising Officer can grant a renewal of an authorisation before it would cease to have effect.
- 5.3.2 An application for a renewal must not be made more than seven days before the authorisation is due to expire.
- 5.3.3 A renewal can last for up to three months, effective from the date that the previous authorisation would ceased to have effect.
- 5.3.4 An Authorising Officer can grant more than one renewal as long as the request for authorisation still meets the requirements for authorisation. An Authorising Officer must still consider all of the issues that are required for a first application before a renewal can be granted.
- 5.3.5 If the reason for requiring authorisation has changed from its original purpose it will not be appropriate to treat the application as a renewal. The original authorisation should be cancelled and a new authorisation should be granted.
- 5.3.6 An application for a renewal must be completed on the appropriate form. For DS please use the form marked "rends" in Appendix B and for CHIS please use the form marked "renchis" in Appendix B.

5.3.7 The Authorising Officer should keep a copy of the renewal and a copy should be given to the Investigating Officer. A copy of the renewal form must also be sent to the RIPA co-ordinator.

## **5.4 Cancellations**

5.4.1 If the reason for requiring the authorisation no longer exists, the authorisation **must** be cancelled and in any event as soon as the operation for which an authorisation was sought ceases to be necessary or proportionate. This applies to both original applications and renewals.

5.4.2 Authorisations **must** also be cancelled if the surveillance has been carried out and the original aim has been achieved. Authorising Officers will ensure that authorisations are set to expire at the end of the appropriate statutory period.

5.4.3 An authorisation can be cancelled by using form marked "cands" in Appendix B for DS and the form marked "canchis" in Appendix B for CHIS. An Investigating Officer should complete the details required on the first page, sections 1 and 2 of the cancellation form. The form should then be submitted to the Authorising Officer who will complete sections 3, 4 and 5.

5.4.4 It is the responsibility of the Investigating Officer to monitor their authorisations and cancel them where appropriate.

5.4.5 The Authorising Officer should keep a copy of the cancellation form and a copy should be given to the Investigating Officer. A copy of the cancellation form must also be sent to the RIPA co-ordinator.

## **5.5 Review of Policy and Procedure**

i The Economy and Business Improvement Overview & Scrutiny Committee will receive reports following the use of RIPA. Those reports will contain information on;

- Where and when the powers had been used
- The objective
- The authorisation process
- The job title of the authorising officer
- The outcome including any legal court case
- Any costs

ii The Corporate Governance Group will review the use of the RIPA and report to Economy and Business Improvement Overview & Scrutiny Committee on an annual basis

## **6 THE RIPA CO-ORDINATOR**

### **6.1 Role**

All original applications for authorisations and renewals including those that have been refused must be passed to the RIPA co-ordinator as soon as possible after their completion with copies retained by the Authorising Officer and the Applicant.

All cancellations must also be passed to the RIPA co-ordinator.



**6.1.2** The RIPA co-ordinator will: -

- i. Keep the copies of the forms for a period of at least 3 years;
- ii. Keep a register of all of the authorisations, renewals and cancellations; and
- iii. Keep a database for identifying and monitoring expiry dates and renewal dates.
- iv. Assistant directors, Service managers, Authorising officers, Investigating officers and the RIPA coordinator must ensure that any electronic and paper records relating to a RIPA investigation are used, retained or destroyed in line with the councils policies, Data Retention schedules and the Data Protection Act 1998.
- v. Provide administrative support and guidance on the processes involved
- vi. not provide legal guidance or advice
- vii. Monitor the authorisations, renewals and cancellations so as to ensure consistency throughout the Council;
- viii. Monitor each department's compliance and act on any cases of non compliance;
- ix. Provide training and further guidance on and awareness of RIPA and the provisions of this Guide; and
- x. Review the contents of the Guide.

**6.3** It is however the responsibility of the Investigating Officer, the Authorising Officer and the Senior Responsible Officer to ensure that: -

- i. Authorisations are only sought and given where appropriate;
- ii. Authorisations are only sought and renewed where appropriate;
- iii. Authorisations are cancelled where appropriate; and
- iv. They act in accordance with the provisions of RIPA.

**7.0 Legal advice**

- i. OneLegal will provide legal advice to staff making, renewing or cancelling authorisations
- ii. Requests for legal advice will be in writing and copied to the RIPA co-ordinator to keep on file
- iii. Responses to requests for legal advice will be in writing and copied to the RIPA coordinator to keep on file.

## APPENDIX A

### Officers

The following officers are the Senior responsible officer and the Authorising officers for the purposes of RIPA

#### **Senior Responsible Officer**

Chief Executive Mr A North

#### **Authorising Officers**

Strategic Directors Mrs P Pratley and Mr G Lewis (The 2 Strategic Directors also act as Deputy Chief Executive on a rotation basis. Where the guidance states the Senior Responsible officer and he is unavailable then the Deputy Chief Executive will undertake the duties of the Senior Responsible officer.

Chief Finance Officer Mr M Sheldon

Borough Solicitor and Monitoring Officer Mrs S Freckleton

## APPENDIX B

### AUTHORISATION FORMS

**The authorisation, review and cancellation forms will be the forms that are current on the home page of**

<http://security.homeoffice.gov.uk/ripa/>

**APPENDIX C**  
**REGULATION OF INVESTIGATORY POWERS ACT 2000**  
**CHELTENHAM BOROUGH COUNCIL**  
**AGENT'S AGREEMENT FORM**

I .....(insert Agent's name) of.....  
.....(address) confirm that  
in relation to .....  
.....  
.....  
.....  
.....  
.....  
.....(name or description of the  
surveillance) I agree to comply with the Regulation of Investigatory Powers Act 2000, with  
all statutory provisions, statutory Codes of Practice and with Cheltenham Borough Council's  
Procedural Guide when undertaking any and all surveillance authorised by Cheltenham  
Borough Council under the Regulation of Investigatory Powers Act 2000. I acknowledge  
receipt of a copy of the Council's Authorisation Form reference number  
.....dated the ..... and I agree not to carry out any  
surveillance that is contrary this authorisation.

Signed.....

Dated.....

## APPENDIX D

## Will DCS authorisation be required?

Are you carrying out the surveillance in a way that people are going to be unaware that it is being carried out?	No →	Surveillance is unlikely to be covert and therefore authorisation will not be required
↓ Yes		
Is the surveillance part of a specific investigation?	No →	Unlikely to require authorisation
↓ Yes		
Are you going to be collecting information about a person's private or family life?	No →	Unlikely to require authorisation
↓ Yes		↓ No
Will the surveillance require the presence of an individual or use a surveillance device on a person's premises or private vehicle?	Yes →	This may fall within the definition of intrusive surveillance
↓ No		
You will need to obtain authorisation for D.C.		Seek administrative advice from RIPA co-ordinator and seek legal advice from One legal

### Will CHIS authorisation be required?

Are you carrying out the surveillance in a way that people are going to be unaware that it is being carried out?	No —————→	It is unlikely that the CHIS is covert and authorisation will be required
↓ Yes		
Are you going to establish a personal or other relationship with someone in order to obtain, provide access to, or disclose information as part of that relationship?	No —————→	Unlikely to require authorisation
↓ Yes		
Are you going to be using a vulnerable person or persons under 18 years old?	Yes —————→	Speak to the RIPA co-ordinator and seek advice from One legal before you undertake any surveillance
↓ No		
Is the person establishing a relationship with a CBC employee or agent?		
↓ Yes		
Authorisation for CHIS should be obtained and an agent's agreement form should be completed when an agent is used		