April 2015

Regulation of Investigatory Powers Act (RIPA) Procedural Guide

(Including additional guidance on Non - RIPA surveillance)

CHELTEN
BOROUGH CO

Document History
Document Location S: Library drive

Control Location: Code of Corporate Governance

Review Period: Annual

Reviewed by: Corporate Governance Group

Version Number	Version Date	Summary of Changes
1.0	**16/04/2013**	**Revised Guidance**

This document is owned by:

Name	Job Title	Version
Mark Sheldon	Director Resources	1.1

This document has been distributed to:

Name	Job Title	Version
All CBC employees, Members, and on the Public website		1.0

Index

Forward:

This revised guidance reflects two significant legislative changes.

1. **Approval of RIPA Authorisations by a Justice of the Peace:** The amendments in the Protection of Freedoms Act 2012 mean that the authorisations and notices under RIPA for the use of particular covert techniques can only be given effect once an order approving the authorisation or notice has been granted by a Justice of the Peace (JP).

2. **Directed surveillance crime threshold:** Amendments to the Regulation of Investigatory Powers (Directed Surveillance and Covert Human Intelligence Sources) Order 2010 means that we can only grant an authorisation under RIPA for the use of directed surveillance when investigating particular types of criminal offences. These are criminal offences which attract a maximum custodial sentence of six months or more or criminal offences relating to the underage sale of alcohol or tobacco.

This guidance provides advice on how Cheltenham Borough Council can best approach these changes in law and the new arrangements that need to be put in place to implement them effectively. It is supplementary to the legislation and to the statutory Codes of Practice. If there any doubts about the guidance then the RIPA coordinator or One Legal should be consulted.

This guidance is intended for investigation officers that may use covert techniques, including Environmental Health, Benefit Fraud Officers and Enforcement Officers. However, it will also be of use to authorising officers and designated persons and to those who oversee the use of investigatory techniques including elected members.

Surveillance outside of RIPA
There may be a necessity for the Council to undertake surveillance which does not meet the criteria to use the RIPA legislation such as in cases of serious disciplinary investigations or for overt operations this guidance provides some advice on the process for those situations.

The Council must still meet its obligations under the Human Rights Act and any surveillance outside of RIPA must still be necessary and proportionate having taken account of the intrusion issues. The decision making process and the management of such surveillance must be well documented.

There is also a requirement for the Council's Senior Responsible Officer (SRO) to regularly monitor surveillance outside of RIPA. Therefore before any such surveillance takes place advice must be sought from Legal Services. Guidance is contained within this policy for this type of surveillance.

The Human Rights Act 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.

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

Steve Jordan. Leader.
Cheltenham Borough Council

1 INTRODUCTION

1.1 RIPA presents some difficult judgments which must be made from time to time. Whilst individual services can and do operate their own procedures, this is an issue which affects the Council corporately and staff will never be criticised for seeking advice.

1.2 The first point to emphasise is that any person who is unsure about whether to seek authorisation or unsure about whether to issue an authorisation, must seek immediate advice before acting. For those seeking authorisation, advice may initially be sought from their line manager, but it is always appropriate to seek the advice of a member of One Legal. RIPA is a piece of legislation with serious human rights implications whenever it is engaged. The Council is concerned about an individual's rights, but it is also concerned to guard against serious reputational risk.

1.3 The purpose of this document is to ensure that the Council complies with the Regulation of Investigatory Powers Act 2000 (RIPA).

1.4 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.

1.5 Any covert surveillance will have to be authorised and conducted in accordance with RIPA, the statutory codes of practice (issued in December 2014) 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.

1.6 Covert surveillance will only be used by the Council where it judges such use to be necessary and proportionate to the seriousness of the crime or matter being investigated,

1.7 Before requesting authorisation Investigating Officers will have regard to this document and the statutory Codes of practice issued under section 71 RIPA (current version issued in December 2014). 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 Before authorising covert surveillance Authorising Officers will have regard to this Guide and the statutory Codes of Practice. The Codes of Practice are available from the Home Office, CBC RIPA Co-ordinator and direct from the Office of Surveillance website or the Home Office.

1.9 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. The role of the authorising officer is covered in greater detail within paragraph 4.2 of this doicument.

1.10 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 and how the intrusion should be reduced and managed will need to be recorded within the application form.

1.11 There must be no situation where a council 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.

1.12 Any queries concerning the content of the document should be addressed to the RIPA Co-ordinator (Governance, Risk and Compliance officer CBC).

2 THE REGULATION OF INVESTIGATORY POWERS ACT (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.

2.1.1 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

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

2.2.2 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.

2.2.3 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.

2.2.4 There may however be times when the Council uses 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 RIPA and 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.

2.2.5 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 One Legal before they conduct any surveillance.

2.3 Consequences of not following RIPA

2.3.1 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.

2.3.2 Lawful surveillance is exempted from civil liability.

2.3.3 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

2.4.1 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.

2.4.2 It is important that the Council can show it complies with this Guide and 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 (Local Authorities are not permitted to carry out intrusive surveillance). The information is included in this procedural guide to avoid inadvertent use of intrusive surveillance. Intrusive surveillance is defined in RIPA as surveillance 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)

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

3.1.3 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.

3.1.4 Any car park where Automated Number Plate Recognition (ANPR) is installed for either payment or enforcement purposes or it is intended to use that equipment to monitor a particular vehicle or person beyond that purpose then the use of RIPA legislation should be considered.

3.1.5 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. They may also be inspected by the OSC in respect of that particular operation. This should be pointed out during the instruction and contract stage. The Authorising Officer should ensure that the agents are qualified or have the necessary skills to achieve the objectives. They should also ensure that they understand their obligations under RIPA. If advice is required please contact One Legal.

3.1.6 The flow chart in Table 1 and 2 provides guidance on the council's procedure for making an application to a Justice of the Peace (JP) seeking an order to approve the grant of a RIPA authorisation or Notice.

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 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) S/He covertly uses such a relationship to obtain information or to provide access to any information to another person; or

c) S/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 council who will have day to day responsibility for dealing with the source on behalf of the authority, and for the source's security, (the handler) the investigation officer

• that there will at all times be another officer within the council who will have general oversight of the use made of the source; (controller) i.e. the responsible line manager.

• that there will at all times be an officer within the council 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 council will always contain particulars as laid down by the Covert Human Intelligence Sources codes of practice (current version issued in December 2014)

3.2.4 Legal advice should always be sought where consideration is given to the use of CHIS.

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 (CHIS) you must consult One Legal before authorisation is sought.

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 One Legal.

3.2.9 If you intend to instruct an agent to be 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. They may also be inspected by the OSC in respect of that particular operation. This should be pointed out during the instruction and contract stage. If advice is required please contact either the RIPA Co-ordinator or One Legal.

3.2.10 The flow chart in Table 1 below provides guidance on the council's procedure for making an application to a Justice of the Peace seeking an order to approve the grant of a RIPA authorisation or Notice.

Table 2 is a copy of the guidance provided to JP/Magistrate s on the process for dealing with an application from the council.

Appendix E provides additional information about the process the RIPA application and authorisation process by a JP/Magistrate

Table 1:

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

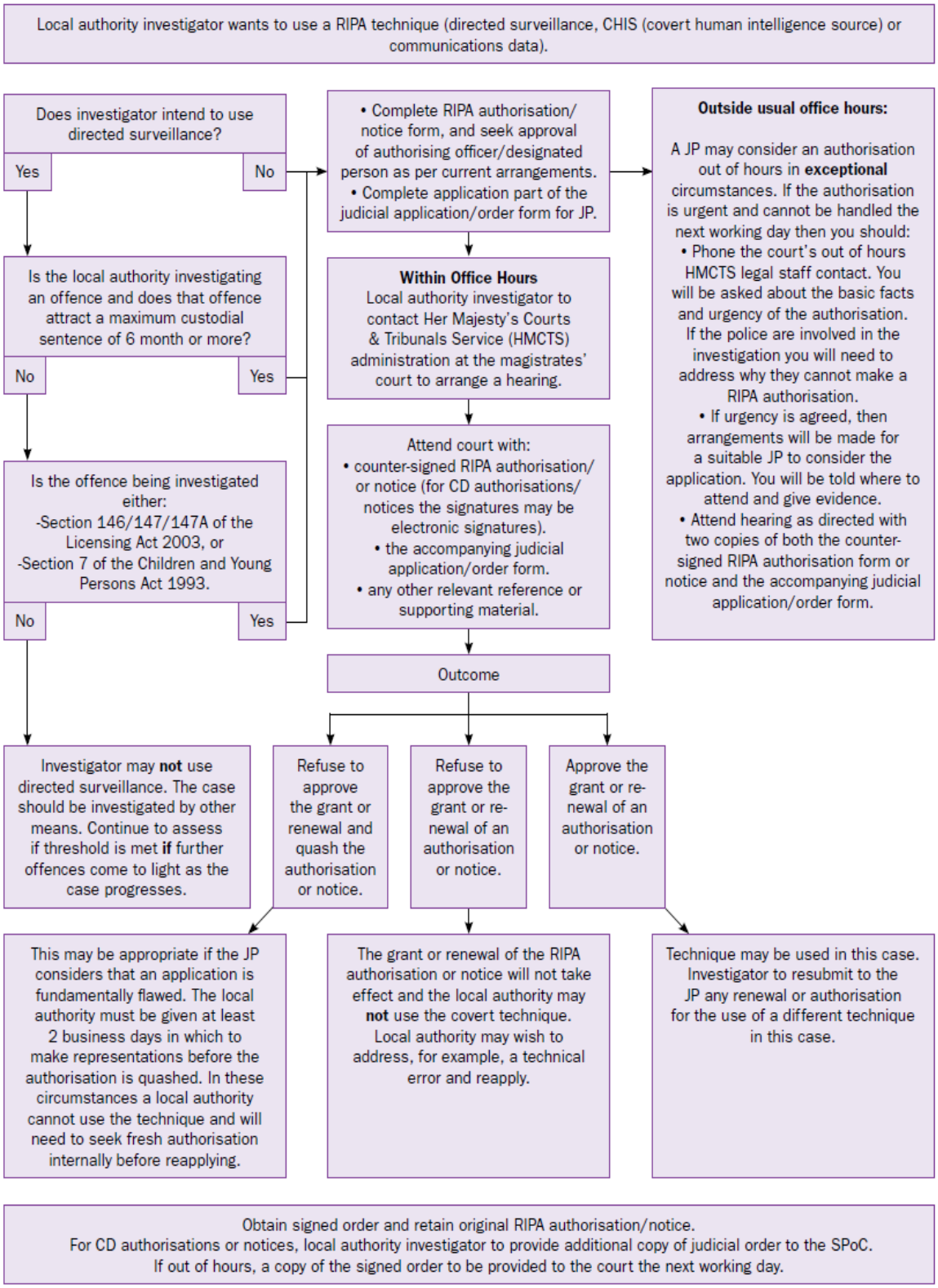

Table 1

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

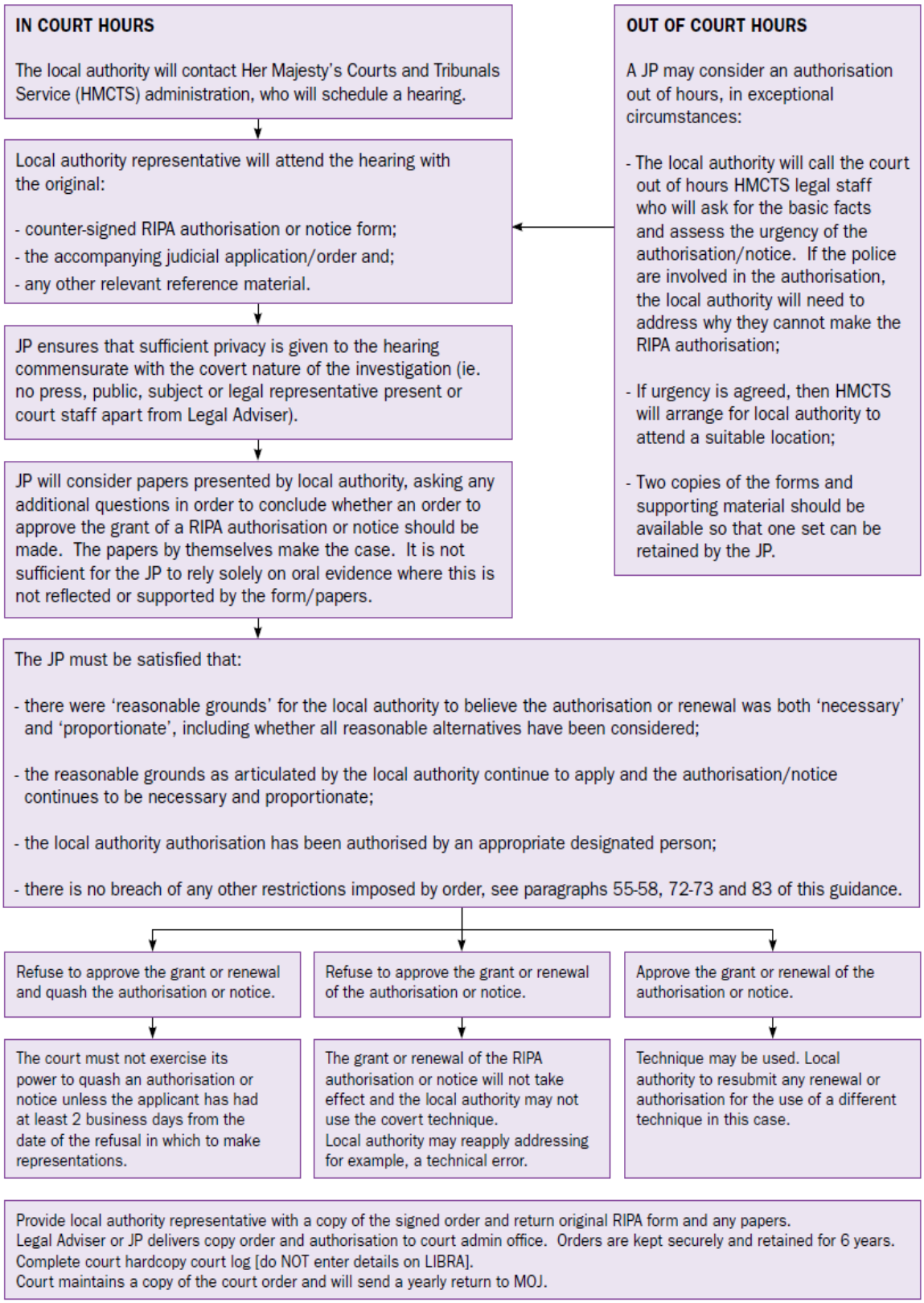

Table 2

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. Operatives will need to be aware of using high powered zoom lenses or CCTV that may fall into this category.

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 One Legal before you undertake any surveillance.

4 PROCEDURE FOR OBTAINING AUTHORISATIONS

4.1 The Senior Responsible Officer:-

Role:

4.1.1 The nominated Executive Director is the Senior Responsible Officer (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 RIPA 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

(g) concerns about the standards of Authorising Officers.

(h) must regularly monitor covert surveillance activity which takes place outside of RIPA as mentioned in the OSC Procedures and Guidance document.

4.2 Authorising Officers

4.2.1 The role of the Authorising Officers is to authorise, review, renew and cancel directed surveillance.

4.2.2 Authorising Officers should not be responsible for authorising investigations or operations in which they are directly involved. Where an Authorising Officer authorises such an investigation or operation the Central Record of Authorisations should highlight this and it should be brought to the attention of a Commissioner or Inspector during their next inspection.

4.2.3 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.

4.2.4 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 Director level.

4.2.5 Authorisations must be given in writing by the Authorising Officer. They must complete the relevant section on the application form and explain exactly what they are authorising, against who, in what circumstances, where etc. It is important that this is very clear as the surveillance operatives are only allowed to carry out what is authorised. This will assist with avoiding errors. They must believe the surveillance is **proportionate** to what it seeks to achieve, taking into account the **collateral intrusion** issues, and that the level of the surveillance is appropriate to achieve the objectives.

4.2.6 If any equipment such as covert cameras, video cameras is to be used, the Authorising Officer should know the capability of the equipment before Authorising its use. This will have an impact on collateral intrusion, necessity and proportionality. They should not rubber-stamp a request. It is important that they consider all the facts to justify their decision. They may be required to justify their actions in a court of law or some other tribunal.

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

4.2.8 Authorised Officers must acquaint themselves with the relevant Codes of Practice issued by the Home Office regarding RIPA (current version issued December 2014 and the latest Procedures and Guidance from the Office of Surveillance Commissioner (OSC). This latter document details their latest guidance to be followed and Authorising Officers are required to hold their own copy.

4.3 Authorising Officers – What you need to do before authorising surveillance

4.3.1 Before giving authorisation an Authorising Officer **must** be satisfied that the reason for the request is for the **prevention and detection of crime and that** the crime attracts a custodial sentence of a maximum of 6 months or more (Table 1 page 11), or is an offence relating to the underage sale of alcohol or tobacco under sections 146, 147 or 147A of the Licensing Act 2003 or section 7 of the Children and Young Persons Act 1933. 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.

- 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

4.3.2 An Authorising Officer **must** also be satisfied the surveillance in each case is **necessary** and **proportionate in those particular circumstances and demonstrate by completing the relevant section of the authorisation how they reached their decision.**

Nessity and Proportionality are 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 which, for Local Authorities is the **prevention and detection of crime and that** the crime attracts a custodial sentence of a maximum of 6 months or more or for the purpose of preventing or detecting specified criminal offences relating to the underage sale of alcohol and tobacco The applicant and Authorising Officers must also be able to demonstrate that there were no other means of obtaining the same information in a less intrusive method.

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 explaining proportionality the Authorising Officer should explain why the methods and tactics to be adopted during the surveillance is not disproportionate.

4.3.3 The codes provide guidance relating to proportionality which should be considered by both applicants and Authorising Officers:

- balancing the size and scope of the proposed activity against the gravity and extent of the perceived crime or offence;
- explaining how and why the methods to be adopted will cause the least possible intrusion on the subject and others;
- considering whether the activity is an appropriate use of the legislation and a reasonable way, having considered all reasonable alternatives, of obtaining the necessary result;
- evidencing, as far as reasonably practicable, what other methods had been considered and why they were not implemented.

4.3.4 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. They should also detail the exact activity being authorised, who against etc. in the relevant authorisation section on the form.

4.3.5 The applicant will now be required to complete the relevant forms and attend Magistrates' Court to seek a JP's approval (see Appendices D,E or F on the RIPA Application and Authorisation Process)
Appendix G provides the contact details for Her Majesty's Courts and Tribunal Service

4.4 Investigating Officers – What you need to do before applying for authorisation

4.4.1 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.

4.4.2 Appendix E provides guidance on the full application and authorisation procedure, including the application process to seek approval from a Justice of the Peace. This should be read by all staff.

4.4.3 The applicant or some other person must carry out a feasibility study as this may be required to be seen by the Authorising Officer. The person seeking the authorisation should then complete the application form having regard to the guidance given in this Guide and the statutory Codes of Practice.

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

5 DURATION, REVIEW, RENEWAL AND CANCELLATION OF AUTHORISATIONS

5.1 Duration

5.1.1 Directed Surveillance (DS) authorisations will cease to have effect after three months from the date of approval by the magistrate unless renewed or cancelled. They do not expire, they must be cancelled when the surveillance is no longer proportionate or necessary.

5.1.2 Authorisations should be given for the maximum duration but reviewed on a regular basis and formally cancelled when no longer needed.

5.1.3 CHIS authorisations will cease to have effect after twelve months from the date of approval.

5.1.4 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

5.1.5 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 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. The original copy of the review form must also be sent to the RIPA Co-ordinator.

5.3 Renewals

5.3.1 An Investigating Officer must ask an Authorising Officer to grant a renewal of an authorisation before it would cease to have effect. The approval of a Justice of the Peace (JP) is required prior to undertaking any covert activity as detailed within the renewal form (Appendix B) authorised by the Authorising Officer for a renewal to take affect.

5.3.2 Applications for renewals should not be made until shortly before the original authorisation period is due to expire but the applicant must take account of factors which may delay the renewal process (e.g. intervening weekends or the availability of the relevant Authorising Officer and a JP to consider the application).

5.3.3 Applications for renewal must not be made more than 3 working days before the authorisation is due to expire.

5.3.4 A renewal can last for up to three months, effective from the date that the previous authorisation would ceased to have effect.

5.3.5 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. Each renewal will need the approval of a JP.

5.3.6 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.

5.3.7 An application for a renewal must be completed on the appropriate form. Appendix B

5.3.8 The Authorising Officer and applicant should retain a copy of the renewal and the judicial application / order form. A copy of the original renewal form and the judicial application/order form must also be sent to the RIPA Co-ordinator for the Central Register

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.

5.4.3 As soon as the decision is taken that directed surveillance should be discontinued, the applicant or other investigating officer involved in the investigation should inform the Authorising Officer. The Authorising Officer will formally instruct the investigating officer to cease the surveillance, noting the time and date of their decision. This will be required for the cancellation form Appendix B. The date and time when such an instruction was given should also be recorded in the central record of authorisations.

5.4.4 The Investigating Officer submitting the cancellation should complete in detail the relevant sections of the form and include the period of surveillance and what if any images were obtained and any images containing third parties. The Authorising Officer should then take this into account and issues instructions regarding the management and disposal of the images etc.

5.4.5 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 either cancelled or renewed at the end of the appropriate statutory period.

5.4.3 An authorisation must be cancelled by using the form in Appendix B. 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 and Authorising Officers 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 original cancellation form must also be sent to the RIPA Co-ordinator.

5.4.6 Authorising Officers must review upon cancellation of an application whether or not the objectives were achieved. Any issues identified by the review will be reported to the senior responsible officer.

5.5 Review of Policy and Procedure

i The Audit 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 any use of RIPA and report to Audit Committee on an annual basis.

6 THE RIPA CO-ORDINATOR

6.1 **Role**

6.1.1 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.

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

6.1.3 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 Issue the unique reference number.

iii.. Keep a database for identifying and monitoring expiry dates and renewal dates.

iv. Along with, Directors, Service Managers, Authorising Officers, and the Investigating Officers must ensure that any electronic and paper records relating to a RIPA investigation are used, retained or destroyed in line with the Councils Information Management policies, departmental retention schedules and the Data Protection Act 1998. (DPA)

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.

6.1.4 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 One Legal 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 Reponses to requests for legal advice will be in writing and copied to the RIPA coordinator to keep on file.

8.0 Internet Investigations

8.1 The use of the internet as an investigative method is now becoming routine. However, just because the information being obtained is from the internet staff must still consider all the normal rules and guidance applicable to any type of enquiry conducted within a criminal investigation, such as, the Data Protection Act (DPA), Criminal Procedures Investigations Act (CPIA) and RIPA. In the Surveillance Codes of Practice issued December 2014 there is now a section dealing with these types of enquiries. The paragraph titled Online Covert Activity within the Codes of Practice is replicated below at 8.2 and should be taken into consideration should staff wish to carry out internet open source enquiries, particularly where Social Networking Sites are involved.

8.2 The use of the internet may be required to gather information prior to and/or during an operation, which may amount to directed surveillance. Whenever a public authority intends to use the internet as part of an investigation, they must first consider whether the proposed activity is likely to interfere with a person's Article 8 rights, including the effect of any collateral intrusion. Any activity likely to interfere with an individual's Article 8 rights should only be used when necessary and proportionate to meet the objectives of a specific case. Where it is considered that private information is likely to be obtained, an authorisation (combined or separate) must be sought as set out elsewhere in this code. Where an investigator may need to communicate covertly online, for example, contacting individuals using social media websites, a CHIS authorisation should be considered.

8.3 If staff wish to conduct internet enquiries, particularly Social Networking Sites they must consider the intrusion issues on the subject of the enquiries and other innocent people (collateral intrusion) and when obtaining the evidence this must be stored in line with the Data Protection Act. They must also consider whether they are monitoring in line with the surveillance definition. If so, and they are likely to obtain private information they are likely to require authorisation under the RIPA legislation. These activities are forming part of the RIPA inspections and will also be audited internally.

9.0 Reporting Errors

9.1 There is no a requirement to report all covert activity that was not properly authorised to the OSC in writing as soon as the error is recognised. This would be known as an error. This includes activity which should have been authorised but wasn't or which was conducted beyond the directions provided by the authorising officer. It is therefore important that when an error has been identified it is brought to the attention of the SRO in order to comply. This will require a report detailing any remedial action taken. The Council also has a responsibility to report to the Inspector at the commencement of an inspection all activity which should have been authorised but wasn't. This is to confirm that any direction provided by the Chief Surveillance Commissioner has been followed. This will also assist with the oversight provisions of the Councils' RIPA activity.

9.2 This does not apply to covert activity which is deliberately not authorised because an authorising officer considers that it does not meet the legislative criteria, but allows it to continue. This would be surveillance outside of RIPA. ***Urgent Authorisations***

As from 1 November 2012 there is no provision under RIPA for urgent oral authorisations

10.0 Surveillance Outside of RIPA

10.1 Amendments to the Regulation of Investigatory Powers (Directed Surveillance and Covert Human Intelligence Sources) Order 2010 mean that a local authority can now only grant an authorisation under RIPA where the local authority is investigating criminal offences which attract a maximum custodial sentence of at least six months or criminal offences relating to the underage sale of alcohol or tobacco.

10.2 As a result of the changes in legislation, it is envisaged that surveillance may be required which falls outside of RIPA (for example in the case of anti-social behaviour offences which do not attract a maximum custodial sentence of at least six months imprisonment). The Office of Surveillance Commissioners Procedures and Guidance 2011 states that it is prudent to maintain an auditable record of decisions and actions to use covert surveillance without the protection of RIPA and that such activity should be regularly reviewed by the SRO. The SRO will therefore maintain an oversight of non RIPA surveillance in her role as SRO to ensure that such use is compliant with Human Rights legislation. The RIPA Monitoring Officer will maintain a central record of non RIPA surveillance.

10.3 As part of the new process of formally recording and monitoring non RIPA surveillance, a non RIPA surveillance application form (see appendix H) should be completed and authorised by at least a tier 4 level manager. A copy of the non RIPA surveillance application form can be found on the Intranet or is available from the RIPA Monitoring Officer.

10.4 Non RIPA surveillance also includes staff surveillance which falls outside of RIPA. Any surveillance of staff must be formally recorded on the non-RIPA surveillance Application Form and authorised by the Head of Service in consultation with the Head of Internal Audit. A central record of staff surveillance is also maintained by the SRO.

11.0 Equipment

11.1 All equipment capable of being used for Directed Surveillance such as cameras etc. should be for their purpose by the Authorising Officer, fit for purpose for which they are intended. The equipment should be logged on the central register of equipment held by the RIPA Co-Ordinator. This will require a description, Serial Number, an explanation of its capabilities.

11.2 When completing an Authorisation the applicant must provide the Authorising Officer with details of any equipment to be used and its technical capabilities. The Authorising Officer will have to take this into account when considering the intrusion issues and proportionality. The Authorising Officer must make it clear on the Authorisation exactly what equipment if any they are authorising and in what circumstances.

12.0 Joint Agency Surveillance

12.1 In cases where one agency is acting on behalf of another, it is usually for the tasking agency to obtain or provide the authorisation. For example, where surveillance is carried out by Council employees on behalf of the Police, authorisation would be sought by the Police. If it is a joint operation involving both agencies the lead agency should seek authorisation.

12.2 Council staff involved with joint agency surveillance are to ensure that all parties taking part are authorised on the authorisation page of the application form to carry out the activity. When staff are operating on another organisation's authorisation they are to ensure they see what activity they are authorised to carry out and make a written record. They should also provide a copy of the authorisation to the RIPA Monitoring Officer. This will assist with oversight of the use of Council staff carrying out these types of operations.

APPENDIX A

Designated Officers

The following officers are the Senior Responsible Officer and the Authorising Officers for the purposes of RIPA

Senior Responsible Officer

Executive Director Pat Pratley

Authorising Officers

Chief Executive; Andrew North, Director Resources; M Sheldon.
Where the guidance states the Senior Responsible Officer but is unavailable then the Chief Executive will undertake the duties of the Senior Responsible Officer.

RIPA Co-ordinator
Corporate Governance, Risk and Compliance Officer. B Parsons

APPENDIX B

AUTHORISATION FORMS

All of the forms necessary for RIPA are available from the Home Office website.

www.gov.uk/government/collections/ripa-forms--2

These forms are a mandatory part of the process and must be used in line with the guidance.

All decisions about using regulated investigatory powers must be recorded as they are taken on the required form.

This is the case for:

- applicants seeking authority to undertake regulated conduct
- Authorising Officers and designated persons who consider and decide whether to grant authority or give notice for that conduct

Select the form that you require from the hyperlinked lists below;

Directed Surveillance

1. Application for the use of directed surveillance
2. Renewal of directed surveillance
3. Review of the use of directed surveillance
4. Cancellation of the use of directed surveillance

Covert Human Intelligence Sources

5. Application for the use of covert human intelligence sources
6. Renewal of authorisation to use covert human intelligence sources
7. Reviewing the use of covert human intelligence sources
8. Cancellation of covert human intelligence sources

Reporting errors to the IOCCO

9. Reporting an error by a CSP to the IOCCO
10. Reporting an error by a public authority to the IOCCO

APPENDIX C

REGULATION OF INVESTIGATORY POWERS ACT 2000

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

Particulars to be contained in records when a COVERT HUMAN INTELLIGENCE SOURCE (CHIS) is used.

The following matters are specified for the purposes of paragraph (d) of section 29(5) of the 2000 Act (which must be included in the records relating to each CHIS):

(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;

(j) all contacts or communications between the source and a person acting on behalf of any relevant investigating authority;

(k) the information obtained by each relevant investigating authority by the conduct or use of the source;

(l) any dissemination by that authority of information obtained in that way; and

(m) 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.

In addition, records or copies of the following, as appropriate, should be kept by the relevant authority:

(a) a copy of the authorisation together with any supplementary documentation and notification of the approval given by the Authorising Officer;

(b) a copy of any renewal of an authorisation, together with the supporting documentation submitted when the renewal was requested;

(c) the reason why the person renewing an authorisation considered it necessary to do so;

(d) any authorisation which was granted or renewed orally (in an urgent case) and the reason why the case was considered urgent;

(e) any risk assessment made in relation to the source;

(f) the circumstances in which tasks were given to the source;

(g) the value of the source to the investigating authority;

(h) a record of the results of any reviews of the authorisation;

(i) the reasons, if any, for not renewing an authorisation;

(j) the reasons for cancelling an authorisation.

(k) the date and time when any instruction was given by the Authorising Officer to cease using a source.

The records kept by public authorities should be maintained in such a way as to preserve the confidentiality of the source and the information provided by that source. There should, at all times, be a designated person within the relevant public authority who will have responsibility for maintaining a record of the use made of the source.

APPENDIX E

RIPA Application and Authorisation Process

As from 1 November 2012 two significant changes came into force that effects how local authorities use RIPA.

- **Approval of Authorisations under RIPA by a Justice of the Peace**: The amendments in the Protection of Freedoms Act 2012 mean that the council's authorisations under RIPA for the use of Directed Surveillance or use of Covert Human Intelligence sources (CHIS) can only be given effect once an order approving the authorisation has been granted by a Justice of the Peace (JP). **This applies to applications and renewals only, not reviews and cancellations.**

- **Directed surveillance crime threshold**: Amendments to the Regulation of Investigatory Powers (Directed Surveillance and Covert Human Intelligence Sources) Order 2010 ("the 2010 Order") mean that the council can now only grant an authorisation under RIPA for the use of Directed Surveillance where the council is investigating criminal offences which attract a maximum custodial sentence of six months or more or criminal offences relating to the underage sale of alcohol or tobacco under sections 146, 147 or 147A of the Licensing Act 2003 or section 7 of the Children and Young Persons Act 1933.

- This crime threshold, as mentioned, is only for Directed Surveillance.

Application, Review, Renewal and Cancellation Forms

No covert activity covered by RIPA or the use of a CHIS should be undertaken at any time unless it meets the legal criteria (see above) and has been authorised by an Authorising Officer and approved by a JP/Magistrate as mentioned above. The activity conducted must be in strict accordance with the terms of the authorisation.
The effect of the above legislation means that all applications and renewals for covert RIPA activity will have to have a JP's approval. It does not apply to Reviews and Cancellations which will still be carried out internally.

The procedure is as follows;

All applications and renewals for Directed Surveillance and use of a CHIS will be required to have a JP's approval.

The applicant will complete the relevant application form ensuring compliance with the statutory provisions shown above. The application form will be submitted to an Authorising Officer for consideration. If authorised, the applicant will also complete the required section of the judicial application/order form (Appendix F)

Although this form requires the applicant to provide a brief summary of the circumstances of the case on the judicial application form, this is supplementary to and does not replace the need to supply the original RIPA authorisation as well. All applications need to be made in consultation with One Legal.

It will then be necessary within Office hours to arrange with Her Majesty's Courts & Tribunals Service (HMCTS) administration at the Magistrates' Court to arrange a hearing. The hearing will be in private and heard by a single JP.

Officers who may present the application at these proceedings will need to be formally designated by the Council under section 223 of the Local Government Act 1972 to appear, be sworn in and present evidence or provide information as required by the JP. If in doubt as to whether you are able to present the application seek advice from One Legal

Upon attending the hearing, the officer must present to the JP the partially completed judicial application/order form, a copy of the RIPA application/authorisation form, together with any supporting documents setting out the case, and the original application/authorisation form.

The original RIPA application/authorisation should be shown to the JP but will be retained by the council so that it is available for inspection by the Commissioners' offices and in the event of any legal challenge or investigations by the Investigatory Powers Tribunal (IPT).

The JP will read and consider the RIPA application/ authorisation and the judicial application/order form Appendix F. They may have questions to clarify points or require additional reassurance on particular matters. These questions are supplementary to the content of the application form**. However the forms and supporting papers must by themselves make the case. It is not sufficient for the council to provide oral evidence where this is not reflected or supported in the papers provided**.

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

The JP may decide to:

Approve the Grant or renewal of an authorisation
The grant or renewal of the RIPA authorisation will then take effect and the council may proceed to use the technique in that particular case.

Refuse to approve the grant or renewal of an authorisation
The RIPA authorisation will not take effect and the council may **not** use the technique in that case.

Where an application has been refused the applicant may wish to consider the reasons for that refusal. If more information was required by the JP to determine whether the application/authorisation has met the tests, and this is the reason for refusal the officer should consider whether they can reapply, for example, if there was information to support the application which was available to the council, but not included in the papers provided at the hearing.

For, a technical error (as defined by the JP/Magistrate), the form may be remedied without going through the internal authorisation process again. The officer may then wish to reapply for judicial approval once those steps have been taken.

Refuse to approve the grant or renewal and quash the authorisation or notice

This applies where the JP refuses to approve the application/authorisation or renew the application/authorisation and decides to quash the original authorisation or notice. However the court must not exercise its power to quash the application/authorisation unless the applicant has had at least 2 business days from the date of the refusal in which to make representations. If this is the case the officer will inform the One Legal who will consider whether to make any representations.

Whatever the decision the JP will record their decision on the order section of the judicial application/order form. The court administration will retain a copy of the council's RIPA application and authorisation form and the judicial application/order form. The officer will retain the original application/authorisation and a copy of the judicial application/order form.

If approved by the JP, the date of the approval becomes the commencement date and the three months duration will commence on this date, the officers are now allowed to undertake the activity.

The original application and the copy of the judicial application/order form should be forwarded to the Central Register and a copy retained by the applicant and if necessary by the Authorising Officer.

The council may only appeal a JP decision on a point of law by judicial review. If such a concern arises, One Legal will decide what action if any should be taken.

All the relevant forms for authorisation through to cancellation must be in writing using the standard forms which are available from the Intranet site, but officers must ensure that the circumstances of each case are accurately recorded on the application form.

If it is intended to undertake both directed surveillance and the use of a CHIS on the same surveillance subject, the respective applications forms and procedures should be followed and both activities should be considered separately on their own merits.

An application for an authorisation must include an assessment of the risk of any collateral intrusion or interference. The Authorising Officer will take this into account, particularly when considering the proportionality of the directed surveillance or the use of a CHIS.

Applications

All the relevant sections on an application form must be completed with sufficient information for the Authorising Officer to consider Necessity, Proportionality and the Collateral Intrusion issues. Risk assessments should take place prior to the completion of the application form. Each application should be completed on its own merits of the case. **Cutting and pasting or using template entries should not take place as this would leave the process open to challenge.**

All applications will be submitted to the Authorising Officer via the Line Manager of the appropriate enforcement team in order that they are aware of the activities being undertaken by the staff. The Line Manager will perform an initial quality check of the application. However they should not be involved in the sanctioning of the authorisation. Completed application forms are to be initialed by Line Managers to show that the quality check has been completed. The form should then be submitted to the Authorising Officer.

Applications whether authorised or refused will be issued with a unique number (obtained from the RIPA Coordinator) by the Authorising Officer, taken from the next available number in the Central Record of Authorisations which is held by the RIPA Coordinator.

If authorised the applicant will then complete the relevant section of the judicial application/order form and follow the procedure above by arranging and attending the Magistrates' Court to seek a JP's approval. (See procedure above RIPA application and authorisation process)

Duration of Applications

- Directed Surveillance 3 Months
- Renewal 3 Months
- Covert Human Intelligence Source 12 Months
- Juvenile Sources 1 Month
- Renewal 12 months

All Authorisations must be cancelled by completing a cancellation form. They must not be left to simply expire. (See cancellations page 16)

Reviews

When an application has been authorised regular reviews must be undertaken to assess the need for the surveillance to continue. The results of a review should be recorded on the central record of authorisations. Particular attention is drawn to the need to review authorisations frequently where the surveillance provides access to confidential information or involves collateral intrusion.

The reviews are dealt with internally by submitting the review form (which is available through the link in appendix B) to the Authorising Officer. There is no requirement for a review form to be submitted to a JP.

In each case the Authorising Officer should determine how often a review should take place. This should be as frequently as is considered necessary and practicable and they will record when they are to take place on the application form. This decision will be based on the circumstances of each application. However reviews will be conducted on a monthly or less basis to ensure that the activity is managed. It will be important for the Authorising Officer to be aware of when reviews are required following an authorisation to ensure that the applicants submit the review form on time.

Applicants should submit a review form by the review date set by the Authorising Officer. They should also use a review form for changes in circumstances to the original application so that the need to continue the activity can be reassessed. However if the circumstances or the objectives have changed considerably, or the techniques to be used are now different a new application form should be submitted and will be required to follow the process again and be approved by a JP. The applicant does not have to wait until the review date if it is being submitted for a change in circumstances.

Service mangers of applicants should also make themselves aware of when the reviews are required to ensure that the relevant forms are completed on time.

Renewal

A renewal form is to be completed by the applicant when the original authorisation period is about to expire but directed surveillance is still required

Should it be necessary to renew a Directed Surveillance or CHIS application/authorisation this must be approved by a JP. The renewal forms can be found by following the links in appendix B

Applications for renewals should not be made until shortly before the original authorisation period is due to expire but the applicant must take account of factors which may delay the renewal process (e.g. intervening weekends or the availability of the relevant Authorising Officer and a JP to consider the application).

The applicant should complete all the sections within the renewal form and submit the form to the Authorising Officer.

Authorising Officers should examine the circumstances with regard to Necessity, Proportionality and the Collateral Intrusions issues before making a decision to renew the activity. A CHIS application should not be renewed unless a thorough review has been carried out covering the use made of the source, the tasks given to them and information obtained. The Authorising Officer must consider the results of the review when deciding whether to renew or not. The review and the consideration must be documented.

If the Authorising Officer refuses to renew the application the cancellation process should be completed. If the AO authorises the renewal of the activity the same process is to be followed as mentioned earlier for the initial application.

A renewal takes effect on the day on which the authorisation would have ceased and lasts for a further period of three months.

Cancellation

The cancellation form Appendix B is to be submitted by the applicant or another investigator in their absence. The Authorising Officer who granted or last renewed the authorisation must cancel it if they are satisfied that the directed surveillance no longer meets the criteria upon which it was authorised. Where the Authorising Officer is no longer available, this duty will fall on the person who has taken over the role of Authorising Officer or the person who is acting as Authorising Officer

As soon as the decision is taken that directed surveillance should be discontinued, the applicant or other investigating officer involved in the investigation should inform the Authorising Officer. The Authorising Officer will formally instruct the investigating officer to cease the surveillance, noting the time and date of their decision. This will be required for the cancellation form. The date and time when such an instruction was given should also be recorded in the central record of authorisations..

The Investigating Officer submitting the cancellation should complete in detail the relevant sections of the form and include the period of surveillance and what if any images were obtained and any images containing third parties. The Authorising Officer should then take this into account and issues instructions regarding the management and disposal of the images etc.

The cancellation process should also be used to evaluate whether the objectives have been achieved and whether the applicant carried out what they stated was necessary in the application form. This check will form part of the oversight function. Where issues are identified they will be brought to the attention of the line manager and the Senior Responsible Officer (SRO). This will assist with future audits and oversight.

Appendix F

Application for judicial approval for authorisation to obtain or disclose communications data, to use a Covert Human Intelligence Source or to conduct directed surveillance. Regulation of Investigatory Powers Act 2000 sections 23A, 23B, 32A, 32B.

Local authority:.....

Local authority department:.....

Offence under investigation:.....

Address of premises or identity of subject:.....

.....
.....

.....
.....

Covert technique requested: (tick one and specify details)

Communications Data ☐

Covert Human Intelligence Source ☐

Directed Surveillance ☐

Summary of details

.....
.....

.....
.....

.....
.....

.....
.....

.....
.....

.....
.....

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

Investigating Officer:.....
....

Authorising Officer/Designated Person:.....

Officer(s) appearing before JP:.....

Address of applicant

department:.....

.....
.....

Contact telephone
number:.....

Contact email address
(optional):.....

Local authority
reference:.....
.

Number of
pages:.....
.....

Order made on an application for judicial approval for authorisation to obtain or disclose communications data, to use a covert human intelligence source or to conduct directed surveillance. Regulation of Investigatory Powers Act 2000 sections 23A, 23B, 32A, 32B.

Magistrates'
court:.....
.....

Having considered the application, (tick one):

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

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

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

Notes

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

Reasons

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

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

Signed:

Date:

Time:

Full name:

Address of magistrates' court:

Appendix G

Contact details for Her Majesty's Courts and Tribunal Service (HMCTS) Gloucestershire

During normal office hours, the court support section should be contacted either by phone or email. There number is 01452 420174 and email is gs-glosmcadmin@hmcts.gsi.gov.uk.

The police have lists of those legal advisers that are contactable out of hours and in the unlikely situation when an application needs to be made urgently details can be obtained from the custody suites at Cheltenham and Gloucester and also the control room at Waterwells.

Appendix H

Non RIPA Surveillance Application Form

Public Authority *(including full address)*		**Unique NO.**	

Name of Applicant		**Department**	

Contact Details	
Investigation/Operation Name (if applicable)	
Investigating Officer (if a person other than the applicant)	

1. DETAILS OF APPLICATION
Describe the purpose of the specific operation or investigation e.g. Internal Disciplinary Investigation. Provide details of the investigation and intelligence case to date to include enquiries already undertaken and their result.
2. DETAILS OF SURVEILLANCE
Describe in detail the surveillance operation to be authorised and expected duration, including any premises, vehicles or equipment (e.g. camera, binoculars, video recording equipment) that may be used. **Explain the information that it is desired to obtain as a result of the directed surveillance.**
3. SUBJECT OF SURVEILLANCE
The identities, where known, of those to be subject of the directed surveillance. **Should include where known name, address, D.O.B. or approximate age.** **If persons unknown please provide any description's or other information that may be known.**
4. MISDEMEANOR UNDER INVESTIGATION
Provide details of what offences or malpractice is under investigation, e.g.. Gross Misconduct against. Disciplinary Regulations.

5. INTRUSION AND PRIVACY ISSUES
Detail whether <u>Confidential Information</u> such as information relating to legal privilege, health, spiritual counselling or other sensitive information is likely to be obtained against any personas a result of the surveillance activity. **Supply details of any <u>Collateral Intrusion</u>.** **Why the intrusion is unavoidable.** **Describe precautions you will take to minimise and manage the collateral intrusion.**
6. NECESSITY AND PROPORTIONALITY
Explain why it is necessary to use the covert methods applied for, can the evidence be obtained by less intrusive methods and explain why this surveillance is proportionate to what it seeks to achieve. How intrusive might it be on the subject of surveillance or on others? And why is this intrusion outweighed by the need for surveillance in operational terms or can the evidence be obtained by any other means?
7. APPLICANTS DETAILS

Name (print)		**Tel No:**	
Grade/Position		**Date Submitted**	
Signature			

<u>AUTHORISATION SECTION</u>
8. AUTHORISED YES OR NO? (see below)
If rejected detail the reason why. **If authorised state exactly what activity is being authorised by whom and if necessary what equipment they are authorised to use and in what circumstances. This should include any specific instructions such as the management of any images which may be obtained. Cover who, what, where, when and how.**
9. NECESSITY AND PROPORTIONALITY
Explain why you believe the surveillance is necessary and proportionate to what is sought to be achieved by carrying out the covert activity.
10. CONFIDENTIAL INFORMATION

If confidential information is likely to be obtained (see box 5) state how the information will be managed and disposed of. (Seek advice from legal section and data controller if required). May require a higher level of authority.
11. DATE OF FIRST REVIEW
Set a review date taking into account all the circumstances. The review date should be no longer than a month to demonstrate that the process is being managed effectively

Date	

12. AUTHORISING OFFICER DETAILS			
Name (Print)		**Grade/Position**	
Signature		**Time and Date**	