CORPORATE POLICY & GUIDANCE DOCUMENT

ON

THE REGULATION OF INVESTIGATORY POWERS ACT 2000

(RIPA)

APRIL 2010

CONTENTS PAGE

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

Acknowledgements:

The Council is grateful to Birmingham City Council and its Chief Legal Officer for allowing the Council to adapt Birmingham City Council's Corporate Policy and Guidance Document on RIPA.

A. Introduction

1. The Human Rights Act 1998 (which brought much of the European Convention on Human Rights and Fundamental Freedom 1950 into UK domestic law) requires the Council, and organisations working on its behalf, pursuant to Article 8 of the European Convention, to respect the private and family life of citizens, his/her home and his/her correspondence.

2. The European Convention did not, however, make this an absolute right, but a qualified right. Accordingly, in certain circumstances, the Council may interfere in the citizen's right mentioned above, if such interference is:-

   (a) **in accordance with the law;**

   (a) **necessary** (as defined in this Document); **and**

   (b) **proportionate** (as defined in this Document).

3. The Regulation of Investigatory Powers Act 2000 ('RIPA') provides a statutory mechanism (i.e. 'in accordance with the law') for authorising **covert surveillance** and the use of a **'covert human intelligence source' ('CHIS')** – e.g. undercover agents. It now also permits public authorities to compel telecommunications and postal companies to obtain and release communications data to themselves in certain circumstances. It seeks to ensure that any interference with an individual's right under Article 8 of the European Convention is necessary and proportionate. In doing so, the RIPA seeks to ensure both the public interest and the human rights of individuals are suitably balanced.

4. The purpose of this guidance is to:

   - explain the scope of RIPA and the circumstances where it applies
   - provide guidance on the authorisation procedures to be followed.

5. The Council has had regard to the Codes of Practice produced by the Home Office in preparing this guidance. If any doubt arises, the Home Office Code of Practice should be consulted; the Code of Practice takes precedence over this guidance.

   CHIS: http://security.homeoffice.gov.uk/ripa/publication-search/general-publications/ripa-cop/covert-human-intel-source-COP?view=Binary

   Covert Surveillance: http://security.homeoffice.gov.uk/ripa/publication-search/general-publications/ripa-cop/covert-surveil-prop-inter-COP?view=Binary

   Communications Data: http://security.homeoffice.gov.uk/ripa/publication-search/general-publications/ripa-cop/acquisition-disclosure-cop?view=Binary

   The codes do not have the force of statute, but are admissible in evidence in any criminal and civil proceedings. Staff should refer to the Home Office Codes of Conduct for supplementary guidance.

6. The authoritative position on RIPA is, of course, the Act itself and any Officer who is unsure about any aspect of this Document should contact, at the earliest possible opportunity, the Council's Head of Governance, for advice and assistance. Appropriate training and development will be organised and training given to the relevant Authorising Officers and other senior managers.

7. The Head of Governance will maintain and check the Corporate Register of all RIPA authorisations, reviews, renewals, cancellations, and rejections. It is the responsibility of

the relevant Authorising Officer, however, to ensure the Head of Governance receives a copy of the relevant Forms within 1 week of authorisation, review, renewal, cancellation or rejection.

8. RIPA and this Document are important for the effective and efficient operation of the Council's actions with regard to covert surveillance and Covert Human Intelligence Sources. Authorising Officers must bring any suggestions for continuous improvement of this Document to the attention of the Head of Governance at the earliest possible opportunity.

9. RIPA forms should be used where **relevant** and they will only be **relevant** where the **criteria** listed on the Forms are fully met.

10. In terms of monitoring e-mails and internet usage, it is important to recognise the important interplay and overlaps with the Council's e-mail and internet policies and guidance, the Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000, the Data Protection Act 1998 and its Codes of Practice. Under normal circumstances, the Council's e-mail and internet policies should be used, as any surveillance is likely to be more relevant under the contract of employment terms as opposed to RIPA.

11. If the correct procedures are not followed, evidence may be disallowed by the courts, a complaint of maladministration could be made to the Ombudsman, and/or the Council could be ordered to pay compensation. Such action would not, of course, promote the good reputation of the Council and will, undoubtedly, be the subject of adverse press and media interest. It is essential, therefore, that all involved with RIPA comply with this Document and any further guidance that may be issued, from time to time, by the Head of Governance.

    RIPA states that:

    "if authorisation confers entitlement to engage in a certain conduct and the conduct is in accordance with the authorisation, then it shall be "lawful for all purposes".

    However, the opposite is not true – i.e. if you do not obtain *RIPA* authorisation it does not make any conduct unlawful (e.g. use of intrusive surveillance by local authorities). It just means you cannot take advantage of any of the special *RIPA* benefits and you may have to justify infringing a person's Human Rights and any evidence you place before the courts may be subject to challenge in respect of the processes used to obtain the evidence (s78 Police and Criminal Evidence Act 1984).

12. **If you are in any doubt on RIPA, this Document or the related legislative provisions, please consult the Head of Governance, at the earliest possible opportunity.**

B. Council Policy Statement

1. The Council takes seriously its statutory responsibilities and will, at all times, act in accordance with the law and take necessary and proportionate action in these types of matters. The Head of Governance will periodically review and update as necessary the Guidance issued in relation to RIPA and may add or substitute officers authorised for the purpose of RIPA.

2. This Corporate Policy and Guidance is based upon the requirements of RIPA and the Home Office's Codes of Practice on Covert Surveillance and Covert Human Intelligence Sources

3. It is the Council's policy that:-

   (a) all covert surveillance/CHIS exercises conducted by the Council should comply with the requirements of RIPA;

   (b) only the authorising officers included on the list maintained by the Head of Governance be permitted to authorise a covert surveillance/CHIS exercise;

   (c) all service areas which may carry out covert surveillance/CHIS exercises are made aware of this Policy and Guidance.

4. Operations under RIPA can be authorised **only** on the following ground:-

   - **For the purpose of preventing or detecting crime or of preventing disorder**

5. In assessing whether or not the proposed surveillance is necessary and proportionate, the authorising officer must consider other appropriate means of gathering the information. The least intrusive method will be considered proportionate by the Courts. Surveillance activity should only be used as a last resort.

C. Authorised Officer Responsibilities

1. It is essential that Directors and Authorising Officers take personal responsibility for the effective and efficient operation of this Document.

2. Certain officers have delegated power to authorise applications under *RIPA*, always provided that the officer is sufficiently removed from the investigation that they can be deemed to manage it but are not involved in its day to day conduct (ie: they **MUST NOT** take part in the surveillance or in the management of the Covert Human Intelligence Source to which the application relates). This will usually allow a delegation down to a level such as Service Delivery Manager.

3. It will be the responsibility of Authorising Officers who have been duly certified to ensure their relevant members of staff are also suitably trained as 'Applicants' so as to avoid common mistakes appearing on Forms for RIPA authorisations.

4. Authorising Officers will also ensure that staff who report to them follow this Corporate Policy & Guidance Document and do not undertake or carry out any form of covert surveillance without first obtaining the relevant authorisations in compliance with this Document.

5. Authorising Officers must also pay particular attention to Health and Safety issues that may be raised by any proposed surveillance activity. Under no circumstances, should an Authorising Officer approve any RIPA form unless, and until s/he is satisfied the health and safety of Council employees/agents are suitably addressed and/or risks minimised, so far as is possible, and proportionate to/with the surveillance being proposed. If an Authorising Officer is in any doubt, s/he should obtain prior guidance on the same from his/her Director, the Council's Health & Safety Officer and/or the Head of Governance.

6. Authorising Officers must acquaint themselves with the relevant Codes of Practice issued by the Home Office regarding RIPA. Any failure to comply exposes the Council to unnecessary legal risks and criticism from the Office of Surveillance Commissioners. Cancellations must be promptly dealt with.

7. Authorising Officers must also ensure that, when sending copies of any Forms to the Head of Governance (or any other relevant authority), the same are sent in **sealed** envelopes and marked '**Strictly Private & Confidential**'.

8. Authorising Officers must ensure that the Leader of the Council is notified of any application for the use of RIPA powers. This can be by way of e-mail notification setting out the following:-

Type of Surveillance: Directed Surveillance or CHIS or Communications Data
Service Area
Purpose of surveillance
Brief details of proposed surveillance.

If the Leader has any issues with the use of RIPA or authorisations granted, these will in the first instance be addressed to the Head of Governance.

9. Authorising Officers must also address the issue of what will happen to the product of the surveillance (i.e. the evidence obtained) and this must be detailed on the form. Where the product of surveillance could be relevant to pending or future criminal or civil proceedings, it should be retained in accordance with established disclosure requirements for a suitable period and subject to review.

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

D. What RIPA Does and Does Not Do

1. **RIPA does**:

- establish a scheme for prior authorisation of directed surveillance.
- prohibit the Council from carrying out intrusive surveillance.
- Compels disclosure of communications date from telecom and postal service providers.
- establish a scheme for the authorisation of the conduct and use of a CHIS.
- provide safeguards for the conduct and use of a CHIS.
- Permit the Council to obtain Communications records from Communications service providers.

2. **RIPA does not**:

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

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

E. Types of Surveillance

1. **'Surveillance'** includes

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

Surveillance can be <u>overt</u> or <u>covert</u>.

2. ***<u>Overt Surveillance</u>***

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

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

4. ***<u>Covert Surveillance</u>***

Covert Surveillance is carried out in a manner calculated to ensure that the person subject to the surveillance is <u>unaware</u> of it taking place. (Section 26(9)(a) of RIPA).

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

6. ***<u>Directed Surveillance</u>***

Directed Surveillance is surveillance which:-

- is <u>covert</u>; and
- is not <u>intrusive surveillance</u> (see definition below – **the Council must not carry out any <u>intrusive</u> surveillance**) or any interference with private property;
- is not carried out in an immediate response to events which would otherwise make seeking authorisation under the Act unreasonable, e.g. spotting something suspicious and continuing to observe it; and

- it is undertaken for the purpose of a **specific investigation** or operation in a manner **likely to obtain private information** about an individual (whether or not that person is specifically targeted for purposes of an investigation). (*Section 26(10) of RIPA).*

7. *Private information* in relation to a person includes any information relating to his private and family life, his home and his correspondence. The fact that covert surveillance occurs in a public place or on business premises does not mean that it cannot result in the obtaining of private information about a person. The definition of private information has been given a wide interpretation by the Courts and will include business information in appropriate circumstances. Prolonged surveillance targeted on a single person will undoubtedly result in the obtaining of private information about him/her and others that s/he comes into contact, or associates, with.

8. Although overt town centre CCTV cameras do not normally require authorisation, if the camera is tasked for a specific purpose, which involves prolonged surveillance on a particular person, authorisation will be required. The way a person runs his/her business may also reveal information about his or her private life and the private lives of others.

9. *Confidential Material* means (a) matters subject to legal privilege; (b) confidential personal information; or (c) confidential journalistic material. Coming across confidential information during a surveillance must be given prior thought before any applications are authorised, as failure to do so may invalidate the admissibility of any evidence obtained. Furthermore, thought must be given before any forms are signed to the retention and disposal of any material obtained under a RIPA authorisation. Where there is any possibility of confidential information being obtained through covert surveillance, the application must be authorised by the Chief Executive, or in his absence, the Corporate Director: Community Protection.

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

   If you think you may obtain confidential material, contact the Head of Governance prior to authorisation.

10. **For the avoidance of doubt, only those Officers designated and certified to be 'Authorising Officers' for the purpose of RIPA can authorise 'Directed Surveillance' IF, AND ONLY IF, the RIPA authorisation procedures detailed in this Document are followed. If an Authorising Officer has not been 'certified' for the purposes of RIPA, s/he can NOT carry out or approve/reject any action set out in this Corporate Policy & Procedures Document.**

11. ***Intrusive Surveillance***

    This is when it:-

    - is covert;

    - relates to residential premises or private vehicles; and

    - involves the presence of a person in the premises or in the vehicle or is carried out by a surveillance device in the premises/vehicle. Surveillance equipment mounted outside the premises will not be intrusive, unless the device consistently provides information of the same quality and detail as might be expected if they were in the premises/vehicle. Merely observing movements from/to a house from a parked vehicle will not be classed as intrusive surveillance.

11. **This form of surveillance can be carried out only by police and other law enforcement agencies**. **Council Officers must not carry out intrusive surveillance. Likewise, the Council has no statutory powers to interfere with private property.**

12. **Employee Surveillance using covert surveillance**

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

However, such surveillance may still potentially be viewed as infringing the employee's right to privacy as established under Article 8 of the Human Rights Act 1998.

Where such surveillance pertaining to a non-criminal investigation into the conduct of any employee is required, officers are required to complete the appropriate form, as if for RIPA but clearly marked as a non-RIPA matter, and then forward the form to their authorising officer for approval.

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

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

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

13. ***Examples of different types of Surveillance***

Type of Surveillance	*Examples*
Overt	- Police Officer or Parks Warden on patrol - Signposted Town Centre CCTV cameras (in normal use) - Recording noise coming from outside the premises after the occupier has been warned that this will occur if the noise persists. - Most test purchases (where the officer behaves no differently from a normal member of the public).
Covert but not requiring prior authorisation	- CCTV cameras providing general traffic, crime or public safety information.
Directed must be RIPA authorised.	- Officers follow an individual or individuals over a period, to establish whether s/he is working when claiming benefit or off long term sick from employment. - Test purchases where the officer has a hidden camera or other recording device to record information which might include information about the private life of a shop-owner, e.g. where s/he is suspected of running his business in an unlawful manner.
Intrusive – **Council cannot do this!**	- Planting a listening or other device (bug) in a person's home or in their private vehicle.

F. Conduct and Use of a Covert Human Intelligence Source (CHIS)

Who is a CHIS?

1. Someone who establishes or maintains a personal or other relationship for the covert purpose of helping the covert use of the relationship to obtain information.

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

2. RIPA does not apply in circumstances where members of the public volunteer information to the Council as part of their normal civic duties, or to contact numbers set up to receive information.

What must be authorised?

3. The Conduct or Use of a CHIS require prior authorisation.

   - **Conduct** of a CHIS = Establishing or maintaining a personal or other relationship with a person for the covert purpose of (or is incidental to) obtaining and passing on information.
   - **Use** of a CHIS = Actions inducing, asking or assisting a person to act as a CHIS and the decision to use a CHIS in the first place.

4. **The Council can use CHIS's IF, AND ONLY IF, RIPA procedures, detailed in this Document are followed. Authorisation for CHIS's can only be granted if it is for the purposes of "preventing or detecting crime or of preventing disorder".**

Juvenile Sources

5. Special safeguards apply to the use or conduct of juvenile sources (i.e. under 18 year olds). **Contact the Head of Governance if considering use of a juvenile source.**

Vulnerable Individuals

6. A Vulnerable Individual is a person who is or may be in need of community care services by reason of mental or other disability, age or illness and who is or may be unable to take care of himself or herself, or unable to protect himself or herself against significant harm or exploitation. A vulnerable individual will only be authorised to act as a source in the most exceptional of circumstances. **Contact the Head of Governance if considering use of a vulnerable source.**

Test Purchases

7. Carrying out test purchases will not (as highlighted above) require the purchaser to establish a relationship with the supplier with the covert purpose of obtaining information and, therefore, the purchaser will not normally be a CHIS. For example, authorisation would not normally be required for test purchases carried out in the ordinary course of business (e.g. walking into a shop and purchasing a product over the counter).

8. By contrast, developing a relationship with a person in the shop, to obtain information about the seller's suppliers of an illegal product (e.g. illegally imported products) will require authorisation as a CHIS. Similarly, using mobile hidden recording devices or CCTV cameras to record what is going on in the shop will require authorisation as directed surveillance. A combined authorisation can be given for a CHIS and also directed surveillance.

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

9. Persons who complain about anti-social behaviour, and are asked to keep a diary, will not normally be a CHIS, as they are not required to establish or maintain a relationship for a covert purpose. Recording the level of noise (e.g. the decibel level) will not normally capture private information and, therefore, does not require authorisation.

10. Recording sound (with a DAT recorder) on private premises could constitute intrusive surveillance, unless it is done overtly. For example, it will be possible to record if the noisemaker is warned that this will occur if the level of noise continues. Placing a stationary or mobile video camera outside a building to record anti social behaviour on residential estates will require prior authorisation.

G. Acquisition of Communications Data

What is Communications Data?

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

Procedure

2. There are two powers granted by s.22 RIPA in respect of the acquisition of Communications Data from telecommunications and postal companies ("Communications Service Provider").

3. S.22(3) provides that any authorised person can authorise another person within the same relevant public authority to collect the data. This allows the local authority to collect the communications data themselves, i.e. if a Communications Service Provider is technically unable to collect the data, an authorisation under this section would permit the local authority to collect the communications data themselves.

4. In order to compel a Communications Service Provider to obtain and disclose, or just disclose Communications Data in their possession, a notice under s.22(4) RIPA must be issued. The sole grounds to permit the issuing of a s.22 notice by a Permitted Local Authority is for the purposes of "**preventing or detecting crime or of preventing disorder**". The issuing of such a notice will be the more common of the two powers utilised, in that the Communications Service Provider will most probably have means of collating and providing the communications data requested.

5. Use of s.22(3) should only be used where the local authority is seeking to collect the information themselves, i.e. either to install its own monitoring system or using its own staff to obtain the information form the Communications Service Provider.
6. Use of s.22(4) should be used when the Communications Service Provider is being required to disclosure or obtain and disclosure the specified information.

7. Once a notice has been issued, it must be sent to the Communications Service Provider. In issuing a notice, the Authorising Officer can authorise another person to liaise with the Communications Service Provider covered by the notice.

8. For the Council Authorising Officers who have been duly authorised by the Head of Governance for the purposes of RIPA may sign the Communications Data forms. Copies of forms must be provided to the Head of Governance within 1 week of signing.

H. Authorisation Procedures

1. Directed surveillance, the use of a CHIS and access to communications data can only be lawfully carried out if properly authorised, and in strict accordance with the terms of the authorisation.

Authorising Officers

2. Forms can only be signed by Authorising Officers who hold a Certificate from the Head of Governance. Authorised posts are listed in **Appendix 1**. This Appendix will be kept up to date by the Head of Governance, and added to as needs require. If a Director wishes to add, delete or substitute a post, s/he must refer such request to the Head of Governance for consideration, as necessary. The Head of Governance has been duly authorised to add, delete or substitute posts listed in **Appendix 1**.

3. Authorisations under RIPA are separate from delegated authority to act under the Council's Scheme of Delegation and internal Portfolio Schemes of Management. All RIPA authorisations, save for authorisations to collect communications data under s.22 (3), are for specific investigations only, they must be reviewed at a minimum at monthly intervals and must be renewed or cancelled once the specific surveillance is complete or about to expire. **The authorisations do not lapse with time!** Authorisations to collect communications data under s.22 (3) have a lifespan of one month. However, they can be renewed by serving a new authorisation or notice for further months, within any time within the current life of the notice. It is the personal responsibility of the authorising officer to ensure that dates are adhered to; it is not the responsibility of the applicant.

Training Records

4. Proper training will be given, or approved by the Head of Governance before Authorising Officers are certified to sign any RIPA Forms. A certificate of training will be provided to the individual and a Central Register of all those individuals who have undergone training or a one-to-one meeting with the Head of Governance on such matters will be kept by the Head of Governance.

5. If the Head of Governance feels that an Authorising Officer has not complied fully with the requirements of this Document, or the training provided to him, the Head of Governance is duly authorised to retract that Officer's certificate and authorisation until s/he has undertaken further approved training or a one-to-one meeting with the Head of Governance.

Application Forms

6. Forms should be accessed via the Home Office website to ensure the latest versions of the forms are used.

Grounds for Authorisation

7. Directed Surveillance or the Conduct and Use of the CHIS and/or disclosure of communications data can be authorised by the Council **only** on the following ground:-

- For the prevention or detection of crime or of preventing disorder

No other grounds are available to local authorities.

Assessing the Application Form

8. Before an Authorising Officer signs a Form, **s/he must**:-

(a) Be mindful of this Corporate Policy & Procedures Document, the training provided by the Head of Governance and any other guidance issued, from time to time, by the Head of Governance on such matters;

(b) The Authorising Officer must ensure proper regard is had to **necessity and proportionality** before any applications are authorised. 'Stock phrases' or cut and paste narrative must be avoided at all times as the use of the same may suggest that insufficient detail has been given to the particular circumstances of any person likely to be the subject of the claim. Any **equipment** to be used in any approved surveillance must also be properly controlled, recorded and maintained for audit purposes.

Satisfy his/herself that the RIPA authorisation is:-

(i) **in accordance with the law**;
(ii) **necessary** in the circumstances of the particular case (that is there is no other reasonably available way to obtain the information) on the ground mentioned in paragraph 7 above; there must be an identifiable offence to prevent or detect; **and**
(iii) **proportionate** to what it seeks to achieve.

(c) The terms contains three concepts:-

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

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

In assessing whether or not the proposed surveillance is proportionate, consider whether there are any other non-intrusive methods, and if there are none, whether the proposed surveillance is no more than necessary to

achieve the objective. **The least intrusive method will be considered proportionate by the courts.** In order to be proportionate, the surveillance must not be excessive by relation to the seriousness of the issue under investigation and there can be no other less intrusive way to discover what is wanted. You must explain the reasons why the method/tactic/technique is not disproportionate and why it is the least intrusive.

The following points should be addressed by the Authorising Officer on the form:-

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

(d) Take into account the risk of intrusion into the privacy of persons other than the specified subject of the surveillance (**Collateral Intrusion**). Measures must be taken wherever practicable to avoid or minimise (so far as is possible) collateral intrusion and the matter is an aspect of determining proportionality; Those carrying out the surveillance should inform the authorising officer if the investigation or operation unexpectedly interferes with the privacy of individuals who are not covered by the authorisation. When the original authorisation may not be sufficient, consideration should be given to whether the authorisation needs to be amended and reauthorised or a new authorisation is required.

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

(e) Set a date for review of the authorisation and review by that date;

(f) Contact Legal Services in order that a check can be made as to any current surveillance (to avoid possible duplication) and so that Legal Services can allocate a Unique Reference Number (URN) for the application as follows:-.

Year/Authorising Officer Code/Number of Application

(g) Ensure that the Leader of the Council is notified of the proposed use of RIPA powers.

(h) Ensure that any RIPA Authorising Officer Register is duly completed, and that a copy of the RIPA Forms (and any review/cancellation of the same) is forwarded to the Head of Governance Central Register, **within 1 week of the relevant authorisation, review, renewal, cancellation, or rejection**.

Additional Safeguards when Authorising a CHIS

9. When authorising the conduct or use of a CHIS, the Authorising Officer **must also:-**

(a) be satisfied that the **conduct** and/or **use** of the CHIS is proportionate to what is sought to be achieved;

(b) be satisfied that **appropriate arrangements** are in place for the management and oversight of the CHIS and this must address health and safety issues through a risk assessment;

(c) consider the likely degree of intrusion of all those potentially affected;

(d) consider any adverse impact on community confidence that may result from the use or conduct or the information obtained; and

(e) ensure **records** contain particulars and are not available except on a need to know basis.

The requirements of s.29(5) RIPA and the Regulation of Investigatory Powers (Source Records) Regulations 2000 (SI: 2000/2725) must be considered and applied when authorising the use of a CHIS. Contact the Head of Governance for advice on the requirements if required.

Urgent Authorisations

10. Urgent authorisations should not normally be necessary. In exceptional circumstances, however, urgent authorisations may be given orally if the time that would elapse before a written authorisation can be granted would be likely to endanger life or jeopardise the investigation or operation for which the authorisation was being given. Contact the Head of Governance if utilising an urgent authorisation. The officer undertaking the surveillance must keep a contemporaneous note of what he/she is authorised to do and actions taken; as must the Authorising Officer. The Authorising Officer must send copies of these notes to the Head of Governance for entry on the Central Register.

Duration

11. The Authorisation **must be reviewed and renewed in the time stated and cancelled** once it is no longer needed. The 'authorisation' to carry out/conduct the surveillance lasts for 3 months (from authorisation) for Directed Surveillance, and 12 months (from authorisation) for a CHIS. However, whether the surveillance is carried out/conducted or not, in the relevant period, does not mean the 'authorisation' is 'spent'. In other words, **the Authorisations do not expire! The authorisations have to be reviewed, renewed and/or cancelled (once they are no longer required)!**

12. Notices/Authorities issued under s.22 compelling disclosure of Communications Data are only valid for one month, but can be renewed for subsequent period of one month at any time.

13. Urgent oral authorisations will cease to have effect after 72 hours, beginning with the time when the authorisation was granted.

14. Authorisations can be renewed in writing when the maximum period has expired. The Authorising Officer must consider the matter afresh, including taking into account the benefits of the surveillance to date, and any collateral intrusion that has occurred.

15. The renewal will begin no later than on the day when the authorisation would have expired. In exceptional circumstances, renewals may be granted orally in urgent cases and last for a period of seventy-two hours. Only authorising officers can give urgent oral authorisation.

1. When some other agency has been instructed on behalf of the Council to undertake any action under RIPA, this Document must be used (as per normal procedure) and the agency advised or kept informed, as necessary, of the various requirements. They must be made aware explicitly what they are authorised to do.

2. When some other agency (e.g. Police, Customs & Excise, Inland Revenue etc):-

   (a) wish to use the Council's resources (e.g. CCTV surveillance systems), that agency must use its own RIPA procedures and, before any Officer agrees to allow the Council's resources to be used for the other agency's purposes, s/he must obtain a copy of that agency's RIPA form for the record (a copy of which must be passed to the Head of Governance for the Central Register); or relevant extracts from the same which are sufficient for the purpose of protecting the Council and the use of its resources

   (b) wish to use the Council's premises for their own RIPA action, the Officer should, normally, co-operate with the same, unless there are security or other good operational or managerial reasons as to why the Council's premises should not be used for the agency's activities. Suitable insurance or other appropriate indemnities may be sought, if necessary, from the other agency for the Council's co-operation in the agent's RIPA operation. In such cases, however, the Council's own RIPA forms should not be used as the Council is only 'assisting' not being 'involved' in the RIPA activity of the external agency.

3. In terms of 2(a), if the Police or other Agency wish to use Council resources for general surveillance, as opposed to specific RIPA operations, an appropriate letter requesting the proposed use, extent of remit, duration, who will be undertaking the general surveillance and the purpose of it must be obtained from the Police or other Agency before any Council resources are made available for the proposed use.

4. A Council Authorising Officer can grant a directed surveillance authorisation to cover both Council and Government Department investigators involved in a joint investigation. Equally a Government Department Authorising Officer can do the same on a joint investigation.

5. The nominated investigator from the organisation with primary responsibility will complete the application, including the names and organisation of all investigators likely to be involved in the surveillance. The Authorising Officer from the lead organisation must make the decision on suitability for surveillance to take place. The Authorising Officer must retain records as described in paragraphs J2 to J4 (Record Management).

6. To ensure that the Authorising Officer is aware of the full facts of the case, the applicant must record the following information on the RIPA form:-

   - That the request for surveillance is part of a joint investigation.
   - Include how many of the officers to be deployed at any one time are investigators from the Council or Government Department.
   - If possible, name the investigators involved.

7. Where joint surveillance is authorised by one organisation (ie the lead organisation), it is good practice for the Investigating Officer/Manager of the other organisation to advise their Authorising Officer of the surveillance activity. This

advice is given so that each authorising officer is aware of all surveillance activity being undertaken by their own investigators, regardless of which organisation authorised the activity.

8. **If in doubt, please consult with the Head of Governance at the earliest opportunity.**

J. Record Management

1. **The Council must keep a detailed record of all authorisations, reviews renewals, cancellations, and rejections, with the Authorising Officers and in a Central Register of all Authorisation Forms, maintained and monitored by the Head of Governance.**

2. ***Records maintained by the Authorising Officers***

The following documents must be retained by the relevant Authorising Officer for such purposes.

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

3. Each form will have a URN. Legal Services will issue the relevant URN to Authorising Officers. The cross-referencing of each URN takes place within the Forms for audit purposes. The relevant Authorising Officer code to be followed is as per **Appendix 1**. Rejected Forms will also have URN's.

Central Register maintained by the Head of Governance

4. Authorising Officers must forward copies of each Form to the Head of Governance for the Central Register, within 1 week of the authorisation, review, renewal, cancellation, or rejection. The Head of Governance will monitor the same and give appropriate guidance, from time to time, or amend this Document, as necessary.

5. The Council will retain records for a period of at least three years from the ending of the authorisation. The Office of the Surveillance Commissioners (OSC) can audit/review the Council's policies and procedures, and individual authorisations.

K. Conclusion

1. Where there is an interference with the right to respect for private life and family guaranteed under Article 8 of the European Convention on Human Rights, and where there is no other source of lawful authority for the interference, or if it is held not to be necessary or proportionate to the circumstances, the consequences of not obtaining or following the correct authorisation procedure set out in RIPA and this Document, may be that the action (and the evidence obtained) will be held to be unlawful by the Courts pursuant to Section 6 of the Human Rights Act 1998.

2. Obtaining an authorisation under RIPA and following this Document, will ensure, therefore, that the action is carried out in accordance with the law and subject to stringent safeguards against abuse of anyone's human rights.

3. Authorising Officers will be suitably trained and they must exercise their minds every time they are asked to sign a Form. They must never sign or rubber stamp Form(s) without thinking about their personal and the Council's responsibilities.

4. Any boxes not needed on the Form(s) must be clearly marked as being 'NOT APPLICABLE', 'N/A' or a line put through the same. Great care must also be taken to ensure accurate information is used and is inserted in the correct boxes. Reasons for any refusal of an application must also be kept on the form and the form retained for future audits.

5. For further advice and assistance on RIPA, please contact the Council's Head of Governance (who is also the Monitoring Officer).

Appendix 1 – List of Authorising Officer Posts

	Authorising Officer Code
Chief Executive	**CEX**
Public Protection Service Delivery Manager	**PPSDM**
Corporate Director: Active Lifestyles/Adult Care & Support	**CDAL**
Benefits Service Delivery Manager	**BSDM**
Head of Governance	**HOG**
Audit & Risk Service Delivery Manager	**ARSDM**

IMPORTANT NOTES

A. **Even if a post is identified in the above list the persons currently employed in such posts are not authorised to sign RIPA Forms (including a renewal or cancellation) unless s/he has been certified by the Head of Governance to do so.**

B. **Only the Chief Executive (or Corporate Director: Active Lifestyles/Adult Care & Support in his/her absence) is authorised to sign Forms relating to Juvenile Sources and Vulnerable Individuals (see paragraph F of this Document) or where there is any possibility of confidential information being obtained.**

C. **If a Director wishes to add, delete or substitute a post, s/he must refer such request to the Head of Governance for consideration, as necessary.**

D. **If in doubt, ask the Head of Governance BEFORE any directed surveillance and/or CHIS is authorised, renewed, rejected or cancelled.**