Stockton-on-Tees Borough Council

Corporate Policy on

The Regulation of Investigatory Powers Act 2000

(RIPA)

Ged Morton
Director, Corporate Services (and Monitoring Officer, Senior Responsible Officer (SRO))
Dunedin House, Columbia Drive, TS17 6BJ
Tel: 01642 527003
Email: Ged.morton@stockton.gov.uk

Martin Skipsey
SRO Support Officer
Assistant Director Procurement and Governance
Tel: 01642 526364
Email: Martin.skipsey@stockton.gov.uk

Version Date: 30 July 2004
Revision: April 2006
Revision: July 2007
Revision: July 2009
Revision: August 2009
Revision: August 2010
Revision: November 2010
Revision: July 2011
Revision: March 2012
Revision: May 2012
Revision: January 2013
Revision: March 2014
Revision: April 2014
Revision: May 2015
Revision: September 2015
Revision: August 2017
Revision: July 2018
Revision: July 2023
Revision: January 2024
Revision: January 2021 – Legislative basis added to forms A2, A3, B2 and B3
Revision: February 2021 – Staff Structure and Authorisations updated
Revision: July 2023 - update the Senior Responsible Officer (SRO) and add the SRO Support Officer details
Revision: January 2024 - update roles and responsibilities

Contents

Note

The Regulation of Investigatory Powers Act 2000 ("RIPA") refers to "Designated Officers or Persons". For ease of understanding and application within Stockton-on-Tees Borough Council, this Corporate Policy Document refers to "Authorising Officers". Furthermore, such Officers can only act under RIPA if beforehand they have been duly certified by the relevant Council Corporate Director of Service and notified to the Director of Corporate Services. For the avoidance of doubt, therefore, all references to duly certified Authorising Officers refer to "Designated Officers" under RIPA.

Acknowledgements: The Borough Council is grateful for the very helpful work of Birmingham City Council, Redcar & Cleveland Borough Council and Durham County Council in connection with RIPA policies and procedures.

A. Introduction and key messages

1. This Corporate Policy Document is based upon the requirements of The Regulation of Investigatory Powers Act 2000 ("RIPA") and the Home Office's Code of Practice on Covert Surveillance and Covert Human Intelligence Sources (covert surveillance will be used only rarely and in exceptional circumstances) and related regulations and orders. The Borough Council takes its responsibilities under RIPA and for ensuring that its RIPA procedures are continuously reviewed and improved extremely seriously.

2. 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 Director of Corporate Services for advice and assistance. Appropriate training and development will be organised, and guidance will be provided by or on behalf of the Director of Corporate Services to relevant Authorising Officers and other senior managers.

3. Copies of this Document and related Forms will be placed on the Intranet and Internet, and copies have also been provided electronically to each Authorising Officer.

4. The Director of Corporate Services will maintain and check the Corporate Register of all RIPA authorisations, reviews, renewals, cancellations and rejections. It is the responsibility of all the relevant Authorising Officers, however, to ensure that the Director of Corporate Services receives the original of each of the relevant Forms **within 5 working days of authorisation, review, renewal, cancellation or rejection**.

5. RIPA and this Document are important for the effective and efficient operation of the Borough Council's actions with regard to covert surveillance and Covert Human Intelligence Sources. This Document will, therefore, be kept under annual review by the Director of Corporate Services. Authorising Officers should bring any suggestions for continuous improvement of this Document to the attention of the Director of Corporate Services at the earliest possible opportunity.

6. In terms of monitoring emails and internet usage, it is important to recognise the important interplay and overlaps with the Borough Council's email and internet policies and guidance (which are continuously reviewed and updated), the Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000, the Data Protection Act 12018 and its related guidance and Codes of Practice. Monitoring of internet and email use is the responsibility of the IT Service within the Finance, Transformation and performance. If anomalies are identified the Internal Audit Service and, where appropriate, the Director of Corporate Services, will be notified. RIPA forms should only be used where **relevant,** and they will be only **relevant** where the **criteria** listed on the Forms are fully met. With effect from 5 January 2004 these criteria were restricted solely to authorisations being believed to be necessary for the purpose of preventing or detecting crime or of preventing disorder.

7. Also, with effect from 5 January 2004 local authorities gained new powers and responsibilities under RIPA to access communications data by virtue of the Regulation of Investigatory Powers (Communications Data) Order 2003 ("the 2003 Order") which brought into effect the provisions of Chapter II of RIPA. After the deadline for compliance expires, requests for access to and disclosure of such data will only be able to be made through a designated (in accordance with RIPA and the 2003 Order) Officer who is also a Home Office accredited Single Point of Contact ("SPOC"). The Borough Council will continue to ensure that it has at least one accredited SPOC in place for this purpose. The Director of Corporate Services is the designated Contact Officer for the receipt of and dissemination of guidance on the acquisition of Communications data from the Home Office.

8. Since the 1 November 2012 two significant changes have taken effect regarding the use of RIPA powers. Firstly, before an authorisation for the use of directed surveillance, the use of a Covert Human Intelligence Source, or the acquisition of Communications data, can be implemented, an order will need

to be obtained approving the grant or renewal of an authorisation, or notice from a Justice of the Peace (a district judge or lay magistrate). This new judicial approval process is in addition to the existing authorisation processes under RIPA and described in this Corporate Policy and Procedure Document. The requirements to assess necessity and proportionality, completing the RIPA authorisation/application form, and seeking an Authorising/Designated Officer's approval remain the same. Secondly, a new crime threshold has been introduced in relation to the authorisation of directed surveillance under RIPA. This does not, however, apply to the authorisation of the use of a Covert Human Intelligence Source, or the acquisition of communications data. Where a directed surveillance authorisation is being sought, this can only be authorised to prevent or detect criminal offences that are either punishable, whether on summary conviction or indictment, by a maximum term of at least 6 months imprisonment, or are related to the underage sale of alcohol or tobacco.

9. The introduction of the requirement to obtain judicial approval for Directed Surveillance and the use or conduct of a CHIS means that local authorities are no longer able to orally authorise the use of RIPA techniques. All authorisations must be made in writing and require JP approval. The authorisation cannot commence until this has been obtained.

10. If you are in any doubt on RIPA, this Document or the related legislative provisions, particularly the most recent significant changes, please consult the Director of Corporate Services, at the earliest possible opportunity.

B. Introduction and Key Messages

1. The Borough Council takes its statutory responsibilities extremely seriously and will, at all times, act in accordance with the law and take necessary and proportionate action in these types of matters. In that regard, the Director of Corporate Services, is the Council's Senior Responsible Officer and is duly authorised by the Council to keep this Document up to date and to amend, delete, add or substitute relevant provisions as necessary. For administration and operational effectiveness, the Director of Corporate Services is also authorised to add, substitute or revoke (the authorisation of) Officers authorised for the purpose of RIPA. Details of the Senior Responsible Officer's duties and the role of Elected Members are provided in Section J of this Document.

2. The Borough Council's Constitution empowers the Chief Executive and Chief Officers (the Corporate Directors), in consultation with the Director of Corporate Services to: -

   a. authorise investigations pursuant to the Regulation of Investigatory Powers Act 2000 in accordance with policy and procedures approved for the purpose

   b. ensure the proper recording of authorisations to investigate. In particular to ensure that authorisations are made in a format approved for the purposes of the Act

   c. ensure the proper review and monitoring of authorised investigations at appropriate intervals and as may be directed by the Act

3. This Document was circulated to the RIPA Steering Group in May and June 2004 and to all relevant Chief Officers and other Senior Managers, in draft format, on 18 June 2004. On the 28 July 2004 the Council's Chief Executive, in exercise of his delegated powers, in consultation with the Deputy Leader of the Council: -

   i. approved the Corporate & Policy Procedure Document on RIPA

   ii. having previously authorised the Director of HR, Legal and Communications (now Director of Corporate Services) to do all that is necessary to establish appropriate corporate policies and procedures and ensure all Services implement and comply with the Corporate Policy Document

4. Following an OSC inspection on 16 May 2005 this Document was reviewed and revised in order to reflect the outcome of and feedback from the inspection. The revised version was circulated to all relevant Officers, Senior Managers and the RIPA Steering Group.

5. The Document was further reviewed and revised as a result of the most recent OSC Inspection on 13 June 2007. It was again circulated to relevant Officers, Senior Managers and the RIPA Steering Group. The Intranet and Internet versions were replaced with the revised Document.

6. An initial review and revision of the Document was undertaken in July 2009 prior to the 2009 OSC Inspection. A further review took place after the Inspection.

7. On 20 May 2010 the Council's Cabinet ratified the Document and affirmed the position regarding the Council's Authorising Officers and the Director of Legal and Communications (now Director of Corporate Services) as the Senior Responsible Officer for RIPA.

8. Following the recent OSC Inspection on 2 April 2012, the Document was again reviewed, revised and reported to Cabinet for consideration.

9. The Document was also reviewed and revised in order to reflect the amendments in the Protection of Freedoms Act 2012 which provided that, with effect from 1 November 2012, local authority authorisations and notices under RIPA can only be given effect once an order approving the

authorisation or notice has been granted by a Justice of the Peace; and the amendments to the Regulation of Investigatory Powers (Directed Surveillance and Covert Human Intelligence Sources) Order 2010, which mean that a local authority can only grant a directed surveillance RIPA authorisation where criminal offences are being investigated which attract a maximum custodial sentence of six months or more or relate to the underage sale of alcohol or tobacco.

C. Effective Date of Operation: 1 August 2004 And Authorised Officer Responsibilities

1. The Corporate Policy, Procedures and the Forms provided in this Document became operative with effect from 1 August 2004 and have since been reviewed and revised on a regular basis. **After May 2012 no Forms other than those appended to this Document will be allowable** and any authorisations under the same will become null and void unless otherwise authorised by the Director of Corporate Services. It is essential, therefore, that Chief Officers and Authorising Officers in their Service Groupings, take personal responsibility for the effective and efficient operation of this Document.

2. The Director of Corporate Services will ensure that all Authorising Officers from each Service Grouping are made fully aware of and receive copies of this Document.

3. It will be the responsibility of Authorising Officers to ensure their relevant members of staff are also made fully aware of and suitably trained as "Applicants" in connection with this Document, so as to avoid common mistakes appearing on Forms for RIPA authorisations.

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

5. The procedural advice is intended to provide guidance to first time or infrequent users of RIPA procedures, as well as a useful checklist to the more frequent users.

6. Authorising Officers must also pay particular attention to Health and Safety issues that may be raised by any proposed surveillance activity. Appropriate records of all risk assessments and their conclusions should always be maintained. 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 suitable 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 form from his/her Chief Officer, the Borough Council's Health & Safety Officer and/or the Director of Corporate Services.

7. Authorising Officers must also ensure that, when sending originals of any Forms to the Director of Corporate Services (or any other relevant authority), the same are sent either electronically or in **sealed** envelopes, marked **"Strictly Private and Confidential"**. If sent electronically, they must nevertheless still be signed.

8. Authorising Officers must ensure that requests for access to and disclosure of communications data under RIPA and the Regulation of Investigatory Powers (Communication Data) Order 2003 are made through the Council's Head of Service for Trading Standards and Licensing who is the Council's contact for the NAFN service which is contracted to undertake appropriate communications data.

9. **It is particularly important that all Authorising Officers are aware of and disseminate information and guidance about the new legislative requirements which came into effect on 1 November 2012 regarding approval orders from a Justice of the Peace in relation to all RIPA authorisations/notices and the crime threshold for directed surveillance authorisations which mean that such authorisations can only be granted where certain criminal offences are being investigated.**

D. General information on RIPA

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

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

    a. **in accordance with the law'**

    b. **necessary** (as defined in this Document); and

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

    The Home Office's Code of Practice provides as follows:

    Necessity and proportionality

    i. Obtaining an authorisation under the 2000 Act (RIPA), 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 believes that the authorisation is necessary in the circumstances of the particular case for one or more of the statutory grounds in Section 28(3) of the 2000 Act for directed surveillance.

    ii. 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 be not arbitrary or unfair.

3. The Regulation of Investigatory Powers Act 2000 ("RIPA") provides a statutory mechanism (ie "in accordance with the law") for authorising **covert surveillance** and the use of a **"covert human intelligence source (CHIS)"** – e.g. undercover agents. 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, RIPA seeks to ensure that both the public interest and the human rights of individuals are suitably balanced.

4. Directly employed Council staff and external agencies working for the Borough Council are covered by the Act during the time they are working for the Borough Council. All external agencies must, therefore, comply with RIPA and the work carried out by agencies on the Council's behalf must be properly authorised by one of the Council's designated **Authorising Officers**.

5. If the correct procedures are **not** followed, evidence may be disallowed by the courts, a complaint of maladministration could be made to the Local Government and Social Care Ombudsman, and/or the Council could be ordered to pay compensation. Such action would not, of course, promote the good reputation of the Borough Council and would, undoubtedly, be the subject of adverse press and media interest.(To emphasise this, please refer to the case of R v (1) Raymond Harmes (2) Gary Cranes (2006) EWCA Crim 928 - further information is available from the Director Hof Corporate Services) 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 Director of Corporate Services.

6. More importantly, if the correct procedures are not followed, an authorisation or notice may be rejected by a Justice of the peace. The Home Office has issued guidance in response to the change in the law introducing judicial oversight of local authority use of RIPA. The guidance explains the

changes that have been made and highlights the tests which Justices of the Peace must consider before deciding whether or not to approve an authorisation or notice under RIPA. In particular, it reinforces the unchanged requirements regarding necessity and proportionality. Specifically, the Justice of the Peace must be satisfied that:

- there were reasonable grounds for the local authority to believe the authorisation or renewal was both necessary and proportionate, including whether reasonable alternatives have been considered
- the reasonable grounds as articulated by the local authority continue to apply and the authorisation/notice continues to be necessary and proportionate
- the local authority authorisation has been authorised by an appropriate person
- there is no breach of any other restrictions imposed by order (i.e. the crime threshold under the Regulation of Investigatory Powers (Directed Surveillance and Covert Human Intelligence Sources) Order 2010; the prohibitions on intrusive surveillance and the restrictions relating to vulnerable individuals and legal privilege

7. A flowchart of the procedures to be followed appears at **Appendices 2, 2A and 2B** of the Procedures Document.

E. What RIPA does and does not do

1. RIPA does:

    - require **prior written authorisation** of **directed surveillance (a local authority cannot orally authorise the use of RIPA)**
    - prohibit the Council from carrying out **intrusive surveillance**
    - require written **authorisation** of the conduct and use of a **CHIS (a local authority cannot orally authorise the use of RIPA)**
    - require safeguards for the conduct and use of a **CHIS**

2. RIPA does NOT:

    - make unlawful, conduct which is otherwise lawful
    - prejudice or disapply any existing powers available to the Borough Council to obtain information by any means not involving conduct that may be authorised under this Act. For example, it does not affect the Borough Council's current powers to obtain information from the Land Registry as to the ownership of a property. To illustrate this, please refer to the decision of the Investigatory Powers Tribunal in C and (1) The Police (2) Secretary of State for the Home Department (IPT/03/32/H). Further information regarding the case is available from the Director of Corporate Services. Also refer to section 80(3) of RIPA (general saving for lawful conduct)

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

4. An Authorising Officer or Applicant should also now seek appropriate guidance from the Director of Corporate Services or through the Director of Corporate Services from a relevant Legal Officer, before applying for approval for an authorisation, renewal or notice under RIPA from a Justice of the Peace.

F. Types of Surveillance

1. **"Surveillance"** includes: -

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

   Surveillance can be overt or covert.

2. **Overt Surveillance**

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

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

4. **Covert Surveillance**

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

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

6. **Directed Surveillance**

   Directed Surveillance is surveillance which: -

   - is covert; and
   - is not **intrusive surveillance** (see definition below - the Borough Council **must not** carry out any **intrusive surveillance)**.
   - is not carried out in an immediate response to events which would otherwise make seeking to obtain prior 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 and to aspects of his business and professional life. The fact that covert surveillance occurs in a public place or on business premises does not mean that it cannot result in the obtaining of private information about a person. Prolonged surveillance targeted on a single person will undoubtedly result in the obtaining of private information about him/her **and others** that s/he comes into contact, or associates, with.

8. Similarly, although overt town centre CCTV cameras do not normally require authorisation, if a camera is tasked for a specific purpose, which involves prolonged surveillance on a particular person, then

authorisation will be required. The way a person runs his/her business may also reveal information about his or her private life and the private lives of others.

9. **For the avoidance of doubt, only those Officers designated and certified (and also notified to the Director of Corporate Services 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" (and/or notified to the Director of Corporate Services) for the purposes of RIPA, s/he can NOT carry out or approve/reject any action set out in this Corporate Policy & Procedures Document.**

10. **Only the Chief Executive, and in his absence the Deputy Chief Executive are authorised to sign Forms where through the use or conduct of a CHIS or through directed surveillance, it is likely that knowledge of confidential information will be acquired (matters subject to legal privilege; confidential personal information e.g. medical records and confidential journalistic material).**

11. Intrusive Surveillance

This is when it:

- is covert
- relates to residential premises and 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 or vehicle 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

12. This form of surveillance can be carried out only by police and other law enforcement agencies. Council Officers must not carry out intrusive surveillance.

13. It should be noted however that under section 48(3) of RIPA, Surveillance (and therefore intrusive surveillance) does not include any conduct of a CHIS of obtaining or recording (whether or not using a surveillance device) any information which is disclosed in the presence of the source, or the use of a CHIS for so obtaining or recording information.

14. Examples of different types of Surveillance

Type of Surveillance	**Examples**
Overt - therefore not requiring RIPA authorisation	• Police Officer or Community 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 following an individual or individuals over a period of time, to establish whether s/he is working when claiming benefit or off long-term sick from employment and claiming sick pay • 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 - the Borough Council cannot do this!	• Planting a listening or other device (bug) in a person's home or in their private vehicle • Covert recording in a person's home or in their private vehicle by an authorised CHIS is NOT however surveillance and not therefore intrusive

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

Who is a CHIS?

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

2. RIPA does not apply in circumstances where members of the public **volunteer** information to the Borough Council as part of their normal civic duties, or 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 which 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.

Juvenile Sources

5. Special safeguards apply to the use or conduct of juvenile sources (i.e. under 18-year-olds). On no occasion can a child under 16 years of age be authorised to give information against his or her parents. Only the Chief Executive and in his absence the Deputy Chief Executive are duly authorised by the Borough Council to authorise the use of Juvenile Sources.

Vulnerable Individuals

6. A Vulnerable Individual is a person who is or may be in need of community care services by reason of mental or other disability, age or illness and who is or may be unable to take care of himself or herself, or unable to protect himself or herself against significant harm or exploitation.

7. A Vulnerable Individual will only be authorised to act as a source in the most exceptional of circumstances. Only the Chief Executive and in his absence the Director of Corporate Services are duly authorised by the Borough Council to authorise the use of Vulnerable Individuals.

Test Purchases

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

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

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

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

11. Recording sound (with a DAT recorder) on private premises could constitute intrusive surveillance, unless it is done overtly. For example, it will be possible to record sound 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 or in a building to record anti-social behaviour outside on residential estates will require prior authorisation.

H. Authorisation Procedures

1. **Directed surveillance** and the use of a **CHIS** can only be lawfully carried out if properly authorised, and in strict accordance with the terms of the authorisation. Appendices 2A and 2B of the related procedure document must now be followed for all RIPA authorisations, renewals and notices regarding the requirements for the approval of a Justice of the Peace.

Authorising Officers

2. Forms can only be signed by Authorising Officers who have been certified as an Authorising Officer by their Chief Officer and have been notified to the Director of Corporate Services.

3. Authorisations under RIPA are separate from delegated authority to act under the Council's Scheme of Delegation and internal Service Grouping Schemes of Delegation. RIPA authorisations are for specific investigations only and must be renewed or cancelled once the specific surveillance is complete or about to expire. **The authorisations do not lapse with time!**

Training Records

4. Appropriate guidance or training will be given or approved by or on behalf of the Director of Corporate Services to all Authorising Officers in connection with the Policy Document. A certificate will be provided to, and a Central Register will be kept of all those individuals who have undergone training or received a one-to-one or service group meeting with the Director of Corporate Services.

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

Application Forms

6. Only the approved RIPA forms must be used. Any other forms used, will be rejected by the Authorising Officer and/or the Director of Corporate Services.

7. "A Forms" (Directed Surveillance) -Form A1 Application for Authority for Directed Surveillance

   - Form A2 Review of Directed Surveillance Authority
   - Form A3 Renewal of Directed Surveillance Authority
   - Form A4 Cancellation of Directed Surveillance

8. "B Forms" (CHIS)

   - Form B1 Application for Authority for Conduct and Use of a CHIS
   - Form B2 Review of Directed Surveillance Authority
   - Form B3 Renewal of Directed Surveillance Authority
   - Form B4 Cancellation of Conduct and Use of a CHIS
   - Form B5 Source Record of a CHIS
   - Form B6 Confidential Record of a CHIS

Grounds for Authorisation

8. With effect from 5 January 2004 **Directed Surveillance (A Forms)** or the **Conduct** and **Use** of the **CHIS (B Forms)** can only be authorised by the Borough Council where an Authorising Officer believes that the authorisation is necessary for the purpose of: -

   a. preventing or detecting crime or of preventing disorder and in the case of Directed Surveillance where a criminal offence is being investigated which meets one of the following conditions:

      i. the offence is punishable, whether on summary conviction or on indictment, by a maximum term of at least 6 months of imprisonment, or

      ii. the offence is an offence under:

         - Sections 146, 147 or 147A of the Licensing Act 2003 or
         - Section 7 of the Children and Young Person Act 1933

The Action to be Authorised

9. A full description of the proposed surveillance operation must be provided on the form. Plans should be used wherever possible, and annexed to the form, particularly where camera surveillance is authorised. Plans can be obtained from the Council's intranet at "Maps at Stockton".

Assessing the Application Form

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

   a. be mindful of this Corporate Policy & Procedures Document, the training and/or guidance provided by or on behalf of the Director of Corporate Services and any other advice or guidance issued, from time to time, by the Director of Corporate Services

   b. recognise that s/he should not be responsible for authorising investigations or operations in which they are directly involved, although it is recognised that this may sometimes be unavoidable, especially in the case of small organisations, or where it is necessary to act urgently. Where an Authorising Officer authorises such an investigation or operation the Director of Corporate Services should be advised so that the central record of authorisations can be highlighted to reflect this and the attention of a Commissioner or Inspector can be drawn to it during the next available inspection.

   c. Subject to this, satisfy his/herself that the RIPA authorisation is:

      i. **in accordance with the law**

      ii. **necessary** in the circumstances of the particular case on one of the grounds mentioned in paragraph 9 above; **and**

      iii. **proportionate** to what it seeks to achieve

   d. In assessing whether or not the proposed surveillance is proportionate, consider the seriousness of the matter giving rise to the proposed surveillance (e.g. the potential sanction for the crime in the event of a conviction, and the impact of the crime on individuals etc.) and the importance of taking action in respect of it; the implications of not gathering information about the matter; the effects of the proposed surveillance on the subject of the surveillance and on other persons; compare such effects against the seriousness of the matter and the implications of not taking action; indicating what, if any, other action instead of that proposed, might be taken; and confirming whether the action proposed is likely to be the most effective and the least intrusive

means of obtaining the required information. **The least intrusive method will be considered proportionate by the Courts.**

e. 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 such intrusion and the measures which it is practicable to take to avoid or minimise it, may be an aspect of determining proportionality.

f. Set a date for **review** of the authorisation and review on only that date. Please ensure that the authorisation is reviewed regularly i.e. at least every 4 weeks.

g. Allocate an Authorisation Reference Number (ARN) for the application.

h. Ensure that any RIPA Service Grouping Register is duly completed, and that the original of the RIPA Forms (and any review/cancellation of the same) is forwarded to the Director of Corporate Services' Central Register, **within 5 working days of the relevant authorisation, review, renewal, cancellation or rejection, making sure that they are sent in sealed envelopes, marked "Strictly Private and Confidential".**

Additional Safeguards when Authorising a CHIS

11. 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 of the CHIS or the information obtained; and

e. ensure **records** contain necessary particulars and are not available except on a need-to-know basis. Please refer to Form B6. Also please note that the record keeping requirements in SI 2000/2725 may not be as onerous as they might at first appear. The Authorising Officer may, for instance, be able to justify why, in a particular case, it was not considered necessary to employ three Officers to supervise the case and why it was not considered appropriate to make a record of all of the listed topics, on the grounds that some were inapplicable in the circumstances of the case concerned

Urgent Authorisations

12. Paragraph 3.30 of the Codes of Practice for Covert Surveillance and Property Interference and paragraph 3.26 of the Codes of Practice for CHIS provide that "….. local authorities are no longer able to orally authorise the use of RIPA techniques."

Reviews, Renewals and Cancellations

14. An Authorisation Form must be reviewed in the time stated and cancelled once it is no longer needed. The "authorisation" to carry out/conduct the surveillance lasts for a maximum of 3 months (from authorisation) for Directed Surveillance, and 12 months (from authorisation) for a CHIS. Please note however that authorisations for a juvenile CHIS only last for one month. However, whether the surveillance is carried out/conducted or not, in the relevant period, does not mean the "authorisation" is "spent". In other words, the Forms do not expire! The forms have to be reviewed and/or cancelled (once they are no longer required).

15. Further authorisations can be issued when the maximum period has expired. Prior to that date they can be renewed. The Authorising Officer must consider the matter afresh in both instances, including taking into account the benefits of the surveillance to date, and any collateral intrusion that has occurred. The Justice of the Peace who is asked to consider the relevant application for approval will also consider the matter afresh.

16. A renewal will begin on the day when the original authorisation would have expired.

17. All authorisations will expire at 23.59 hours on the day before the day they were granted. So a directed surveillance authorisation granted at 14.10 hours on 9 June, will expire on 8 September at 23.59 hours.

Justice of the Peace

18. The role of the Justice of the Peace will be to decide whether a local authority grant or renewal of an authorisation or notice to use RIPA should be approved. The authorisation or notice will not come into effect unless and until it is approved by a Justice of the Peace.

19. The role is set out in section 23A RIPA (for Communications Data) and section 32A RIPA (for directed surveillance and CHIS).

20. These sections provide that the authorisation, or in the case of Communications Data, the notice, shall not take effect until the Justice of the Peace has made an order approving such an authorisation or notice. The matters on which the Justice of the Peace needs to be satisfied before giving judicial approval are that:

    - there were reasonable grounds for the local authority to believe that the authorisation or notice was necessary and proportionate and there remain reasonable grounds for believing that these requirements are satisfied at the time when the Justice of the Peace is considering the matter
    - in the case of a CHIS authorisation, that there were reasonable grounds for the local authority to believe that arrangements exist for the safety and welfare of the source that satisfy section 29(5) RIPA and there remain reasonable grounds for believing that these requirements are satisfied at the time when the Justice of the Peace considering the mater
    - in the case of a CHIS authorisation, that there were reasonable grounds for the local authority to believe that the requirements imposed by Regulation of Investigatory Powers (Juveniles) Order 2000 were satisfied and there remain reasonable grounds for believing that these requirements are satisfied at the time when the Justice of the Peace is considering the matter
    - the local authority application has been authorised by a designated person/authorising officer
    - the grant of the authorisation or in the case of Communications Data, the notice was not in breach of any restriction imposed by virtue of an order made under the following sections of RIPA:-
        - 25(3) (for communications data)
        - 29(7)(a) (for CHIS)
        - 30(3) (for directed surveillance and CHIS)

- any other conditions that may be provided for by an order made by the Secretary of State were satisfied

21. The same considerations apply where a local authority is seeking judicial approval to continue using a technique (i.e. a renewal). Although the Justice of the Peace will wish to examine whether the case for a more sustained interference of Article 8 still meets the principle of proportionality. In particular he or she will want to consider the content and value of the information obtained so far.

I. Working with/through other agencies

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

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

   a. wish to use the Borough Council's resources (e.g. CCTV surveillance systems), that agency must use its own RIPA procedures and, before any Officer agrees to allow the Borough 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 Director of Corporate Services for the Central Register) and/or relevant extracts from the same which are sufficient for the purposes of protecting the Borough Council and the use of its resources

   b. wish to use the Borough 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 Borough 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 Borough Council's co-operation in the agency's RIPA operation. In such cases, however, the Borough Council's own RIPA forms should not be used as the Borough Council is only "assisting" and is not "involved" in the RIPA activity of the external agency

3. In terms of 2(a), if the Police or other Agency wish to use Borough 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 Borough Council resources are made available for the proposed use.

4. **If in doubt, please consult with the Director of Corporate Services at the earliest opportunity.**

J. Senior Responsible Officer and Elected Members

The Senior Responsible Officer

1. The Director of Corporate Services is the Council's Senior Responsible Officer.

2. The Home Office Covert Surveillance and Property Interference Revised Code of Practice provides that it is considered good practice that within every relevant public authority, a senior responsible officer should be responsible for:

   - the integrity of the process in place within the public authority to authorise directed surveillance and for the management of CHIS
   - compliance with Part II of RIPA and with this code
   - oversight of the reporting of errors to the relevant Commissioner and the identification of both the cause(s) of errors and the implementation of processes to minimise the repetition of errors
   - engagement with the Commissioner's and inspectors when they conduct their inspections, and
   - where necessary overseeing the implementation of any post inspection action plans recommended or approved by a Commissioner

3. The Code of Practice also provides that within local authorities, the senior responsible officer should be a member of the corporate leadership team and should be responsible for ensuring that all authorising officers are of an appropriate standard in light of any recommendations in the inspection reports prepared by the Officer of Surveillance Commissioners, and that where an inspection report highlights concerns about the standards of authorising officers, the senior responsible officer will be responsible for ensuring the concerns are addressed.

Elected Members

4. The Code of Practice indicates that elected members of a local authority should review the authority's use of the Act and set the Policy at least once a year. They should also consider internal reports on use of the 2000 Act on at least a quarterly basis to ensure that it is being used consistently with the authority's policy and that the policy remains fit for purpose. They should not, however, be involved in making decisions on specific authorisations.

K. Acquisition and Disclosure of Communications Data

Designated Persons or Authorising Officers

1. Designated Persons are defined within RIPA and the 2003. Designated Persons or Authorising Officers may grant an authorisation allowing an Officer of the Authority to collect or retrieve communications data. An authorisation under Section 22(3) of RIPA is granted by the Designated Person or Authorising Officer but must be administered by an Officer of the Council who is a Home Office accredited “SPOC” (a Single Point of Contact). Please, however, see paragraph 20 and the reference to NAFN. Under Section 22(4) of RIPA a notice can be given to a Communications Service Provider requiring them to collect or retrieve the data and produce it to the Council. The notice is given by a Designated Person or Authorising Officer, but must be served by a SPOC.

Authorisations

2. An Authorising Officer may grant an authorisation under Section 22(3) of RIPA to other Officers holding offices, ranks or positions in the Borough Council as defined in the 2003 Order, to engage in any conduct to which Chapter II of RIPA applies.

3. Chapter II applies to:

   (a) any conduct in relation to a postal service or telecommunication system for obtaining communications data, other than conduct consisting in the interception of communications in the course of their transmission by means of such a service or system; and

   (b) the disclosure to any person of communications data

Communications Data

4. Communications Data means any of the following:

   (a) any traffic data comprised in or attached to a communication (whether by the sender or otherwise) for the purposes of any postal service or telecommunications system by means of which it is being or may be transmitted

   (b) any information which includes none of the contents of a communication (apart from any information falling within paragraph (a)) and is about the use made by any person:

      (i) of any postal service or telecommunications service; or

      (ii) in connection with the provision to or use by any person of any telecommunications service, of any part of a telecommunication system

   (c) any information not falling within paragraph (a) or (b) that is held or obtained, in relation to persons to whom he provides the service, by a person providing a postal service or telecommunications service

5. Only Communications Data falling within (b) and (c) above may be authorised or required to be obtained by means of an authorisation given, or notice made on behalf of the Council under Sections 22(3) and (4) of RIPA.

Grounds for Authorisations and Notices

6. An Authorising Officer may only grant an authorisation or give a notice under Sections 22(3) and (4) of RIPA where the Officer believes that it is necessary for the purpose of preventing or detecting crime or of preventing disorder.

Notices

7. Where it appears to an Authorising Officer that a postal or telecommunications operator is or may be in possession of, or be capable of obtaining, any communications data, the Authorising Officer may, by notice to the postal or telecommunications operator, require the operator:

   (a) if the operator is not already in possession of the data, to obtain the data; and

   (b) in any case, to disclose all of the data in his possession or subsequently obtained by him

Proportionality

8. An Authorising Officer must not grant an authorisation or give a notice, unless he believes that obtaining the data in question by the conduct authorised or required by the authorisation or notice is proportionate to what is sought to be achieved by so obtaining the data.

Form and Duration of Authorisations and Notices

9. An authorisation under Section 22(3) of RIPA:

   (a) must be granted in writing or (if not in writing) in a manner that produces a record of its having been granted

   (b) must describe the conduct to which Chapter II of RIPA applies that is authorised and the communications data in relation to which it is authorised

   (c) must specify the matters falling within section 22(2) of RIPA by reference to which it is granted; and

   (d) must specify the office, rank or position held by the person granting the authorisation

10. A notice under Section 22(4) of RIPA requiring communications data to be disclosed or to be obtained and disclosed:

   (a) must be given in writing or (if not in writing) must be given in a manner that produces a record of its having been given

   (b) must describe the communications data to be obtained or disclosed under the notice

   (c) must specify the matters falling within section 22(2) of RIPA by reference to which the notice is given

   (d) must specify the office, rank or position held by the person giving it; and

   (e) must specify the manner in which any disclosure required by the notice is to be made

11. A notice must not require the disclosure of data to any person other than:

   (a) the person giving the notice; or

   (b) such other person as may be specified in or otherwise identified by, or in accordance with, the provisions of the notice but the provisions of the notice shall not specify or otherwise identify a person for the purposes of paragraph (b) unless he holds an office, rank or position with the same relevant public authority as the person giving the notice

12. An authorisation or notice:

    (a) must not authorise or require any data to be obtained after the end of the period of one month beginning with the date on which the authorisation is granted or the notice given; and

    (b) in the case of a notice, must not authorise or require any disclosure after the end of that period of any data not in the possession of, or obtained by, the postal or telecommunications operator at a time during that period

13. An authorisation or notice may be renewed at any time during the end of the period of one month applying to that authorisation or notice.

14. A renewal of an authorisation or of a notice must be by the grant or giving, in accordance with this section, of a further authorisation or notice.

15. Paragraph 12 will have effect in relation to a renewed authorisation or renewal notice as if the period of one month mentioned in that paragraph did not begin until the end of the period of one month applicable to the authorisation or notice that is current at the time of the renewal.

16. All authorisations or renewals also now require the additional approval of a Justice of the Peace before they are effective. Appendices 2A and 2B provide details of the procedure involved and what the Justice of the Peace must be satisfied of if an approval is to be granted.

17. Where an Authorising Officer who has given a notice is satisfied:

    (a) that it is no longer necessary on the relevant grounds falling within section 22(2) of RIPA for the requirements of the notice to be complied with, or

    (b) that the conduct required by the notice is no longer proportionate to what is sought to be achieved by obtaining communications data to which the notice relates, he must cancel the notice

18. The following Communications Data Forms can be found on the RIPA-F-SBC Teams site:

    - ACD 1 Application for Communications Data
    - ACD 2 SPOC Log Sheet
    - ACD 3 Application for Communications Data - SPOC Rejection Form ACD 4 SPOC Officers Report
    - ACD 5 Designated Person's Consideration Form - Application for Communications Data
    - *ACD 6 Notice under Section 22(4) of RIPA
    - *ACD 7 Cancellation of Notice under Section 22(4) of RIPA – Applicant
    - *ACD 8 Cancellation of Notice under Section 22(4) of RIPA - SPOC ACD 9 Schedule for Authorised Acquisition of Subscriber Information

    * These are Stockton-on-Tees Borough Council references

19. Appendix 6 of the related Procedures Document also includes a copy of the Home Office Code of Practice - Acquisition and Disclosure of Communications Data (March 2015).

20. With effect from 1 November 2010 the Council has been using the SPOC facility offered by the National Anti-Fraud Network (NAFN).

L. Records Management

1. General

The Borough Council must keep a detailed record of all authorisations, renewals, cancellations and rejections in Service Groupings and a Central Register of all Authorisation.

Forms will be maintained and monitored by the Director of Corporate Services.

2. Records maintained in Service Groupings

The designated Service Grouping Co-ordinator or Co-ordinators must ensure that the following documents are retained by the relevant Authorising Officer:

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

3. Product from Directed Surveillance

Material obtained as a result of surveillance activities e.g. photographs; video film; surveillance log; officers notes, should be recorded on a record. A copy of this record should be given to the Authorising Officer to be filed with the Authorisation Form. The Applicant or Investigating Officer should retain the original on the case or investigation file. All Officers should ensure that the integrity, security and confidentiality of this material is maintained. Such material should be retained for a period of five years. When it is destroyed, this fact should be recorded on the original record and be signed by the relevant Officer. A copy of the amended record should then be given to the Authorising Officer.

4. Records of Use of and Product from a CHIS

Similarly for Directed Surveillance records, records of the use and of the materials provided by a CHIS should be maintained by the Applicant and Authorising Officer, for a period of five years (see the additional notes on CHIS).

5. Each form will have an ARN. The cross-referencing of each ARN takes place within the Forms for audit purposes. The relevant Service Grouping code should be incorporated into the ARN. Rejected Forms will also have ARNs.

6. Central Register maintained by the Information Governance Team

Authorising Officers must forward the originals of each Form (either electronically, but still signed, or in sealed envelopes, marked “Strictly Private and Confidential”) to the Director of Corporate Services for the Central Register, within 5 working days of the authorisation, review, renewal, cancellation or rejection. The Director of Corporate Services will monitor the same and given appropriate guidance, from time to time, or amend this Document, as necessary.

The Director of Corporate Services and Officers authorised by him will have access to the Central Register, which will be held in a locked filing cabinet.

7. The Borough Council will retain records for a period of at least five years from the ending of an authorisation.

M. Auditing of Authorisations and Records

1. Each service within a Service Grouping which undertakes activities falling within the scope of RIPA, must undertake internal audits of authorisations and records on a quarterly basis. An annual cross cutting audit across Service Groupings will be conducted each year, as directed by the Director of Corporate Services.

2. Quarterly audits should be undertaken by a designated Service Grouping Co-ordinator or an Authorising Officer who in practice undertakes the least number of authorisations for the Service in question. The chosen Auditor should not audit authorisations/renewals/cancellations which he/she has been responsible for. These should be audited periodically (at least once a year by another Authorising Officer in the same service or service grouping).

3. The following should fall within the scope of the audit:

   Applications (including applications for judicial approvals)
   Authorisations
   Risk Assessments
   Reviews and Renewals
   Cancellations
   Records of Product of Directed Surveillance
   Source Records

4. The audit should seek to establish compliance of the authorisations/assessments/reviews/renewals/cancellations and records, with the following: The Regulation of Investigatory Powers Act 2000
   Statutory Instruments made under the Act The Code of Practice on Covert Surveillance
   The Code of Practice on Covert Human Intelligence Sources
   Stockton-on-Tees Borough Council's Corporate Policy and Procedures Documents

   Guidance material issues by The Home Office, LACORS (Local Authority Co-ordinators of Regulatory Services).

5. Each Service should draw up an audit programme. Non-conformities identified as a result of the audit, should be reported to the relevant Service Management Team. Issues of interpretation, which cannot be resolved, should be referred to the Director of Corporate Services.

6. Copies of the service audit should be filed with the management records, held by the Authorising Officers. The cross authority audit report will be held within the Central Record maintained by the Director of Corporate Services.

7. The Office of Surveillance Commissioners (OSC) will audit/review the Borough Council's policies and procedures, and individual authorisations.

N. Complaints

1. Copies of the Codes of Practice on Covert Surveillance and Covert Human Intelligence Sources will be made available to the public by request to the Director of Corporate Services, at the Dunedin House, Columbia Drive TS17 6BJ or by telephoning 01642 527003 or by writing to the Director of Corporate Services, Dunedin House, Columbia Drive TS17 6BJ. Access can also be provided, on request, to the Regulation of Investigatory Powers Act 2000 and related regulations.
2. Complaints about the Council's actions under RIPA should be submitted in writing to the Director of Corporate Services at the above address.
3. Information on the Investigatory Powers Tribunal will be provided as part of the response to any RIPA complaint, including the provision of copies of the Tribunal's complaint form and information leaflet, or by contacting the Director of Corporate Services as indicated above. Alternatively, please refer to the information from the Tribunal's website (www.ipt-uk.com) which is attached following page 32 to this Document.
4. This Corporate Policy Document is available on the Council's website at www.stockton.gov.uk.

N. 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 or 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 Borough 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. Particular care must be taken when considering and confirming whether the proposed surveillance is proportionate to what it seeks to achieve. The explanation must be full and complete. Please refer to paragraph 2 of Section D (General Information on RIPA) and paragraph 11 d in Section H (Authorisation Procedures) for further guidance.

6. Authorising Officers, in giving approval, must state on the form, in detail, why they consider the proposed action to be necessary and proportionate.

7. Care must also be taken to ensure that a full description of the surveillance operation is given on the authorisation form. Appropriate plans, should be used, particularly where camera surveillance is proposed. Such plans can be obtained from the Council's intranet at "Maps at Stockton".

8. This is particularly important in view of the requirements to obtain judicial approval to all authorisations, renewals or notices under RIPA, and to satisfy the crime threshold requirements before any directed surveillance authorisations or renewal is approved.

9. Investigating and Authorising Officers should note that the expiry date (date for cancellation) for an authorisation for three months commencing e.g. on 1 March is 23.59 hours on 31 May and not 1 June.

10. Authorised activities, and therefore all authorisations, should be regularly reviewed i.e. at least every 4 weeks.

11. For further advice and assistance on RIPA, please contact the Borough Council's Director of Corporate Services as the Senior Responsible Officer (who is also the Monitoring Officer). Details are provided on the front of this Document.

Appendix 1

Designated RIPA Co-ordinator and Authorised Officers

RIPA Co-ordinator

The designed RIPA Co-ordinator for Stockton-on-Tees Borough Council under the Regulation of Investigatory Powers Act 2000 will be:

Officer

Mr Ged Morton, Director of Corporate Services

Service Grouping

Corporate Services, Dunedin House, Columbia Drive, TS17 6BJ

Contact details

Tel: 01642 527003

Email: Ged.Morton@stockton.gov.uk

Authorising Officers

The following Officers will be designated as Authorising Officers for the purposes specified on behalf of Stockton-on-Tees Borough Council under the Regulation of Investigatory Powers Act 2000:

Authorising Officer

Marc Stephenson

Service Grouping

Assistant Director - Regulated Services and Transformation

Contact details

Email: marc.stephenson@stockton.gov.uk

Approval to authorise				
Directed Surveillance	Use or Conduct of a Source	Confidential Material	Use of a Vulnerable Individual as a Source	Use of Juvenile as a Source
Yes	Yes	Yes	Yes	Yes