NORTH SOMERSET COUNCIL

CORPORATE POLICY & PROCEDURES DOCUMENT

THE REGULATION OF INVESTIGATORY POWERS ACT (RIPA 2000)

Richard Penska
Deputy Section 151 Officer
North Somerset Council
Town Hall
Weston-super-Mare
BS23 1EL

Tel: 01275 884256
E-mail: Richard.penska@n-somerset.gov.uk
Version Date: August 2012
Revised: December 2012

CONTENT

		Page
A	**Introduction, Key Messages and Why Surveillance is Necessary**	1 – 2
B	**North Somerset Council Policy Statement**	3
C	**Authorised Officer Responsibilities**	4 – 5
D	**General Information on RIPA**	6
E	**What RIPA Does and Does Not Do**	7
F	**Types of Surveillance** • *Overt* • *Covert* • *Directed* • *Private Information* • *Intrusive* • *Property Interference* • *Tracking Devices and Vehicle Tracking Devices* • *Social Networking Sites SNS* • *Employee Surveillance by covert surveillance*	8 -10
G	**Examples of different types of Surveillance**	11
H	**Conduct and Use of a Covert Human Intelligence Source (CHIS)** • *Who is a CHIS* • *What must be authorised* • *Juvenile Sources* • *Vulnerable Individuals* • *Test Purchases* • *Anti-Social Behaviour Activities* • *Covert e-trading*	12 - 14
I	**Authorisation Procedures** *1) Directed Surveillance* *2) Authorised Officers* *3) Grounds for Authorisation* *4) Judicial Approval* *5) Surveillance Request Forms* *6) Assessing the Application Form for Authorisation* · *Necessity and Proportionality* · *Collateral Intrusion* · *Confidential Information* · *Duration of authorisation & frequency of reviews* · *Review dates* · *Central Register updates* · *Form distribution & retention* *7) Additional Safeguards when Authorising a CHIS* *8) Urgent Authorisations* *9) Reviewing an Authorisation* *10) Renewing an Authorisation* 11) *Cancellation of an Authorisation* 12) *Training Records* 13) *Product from surveillance* · *General Principles* · *Retention & destruction*	15 -23
J	**Working with / through Other Agencies** • *using North Somerset Council resources* • *using North Somerset Council premises*	24
K	**Record Management** • *Directorate Records* • *Central Register*	25
L	**Implications for Non-compliance**	26
L	**Concluding Guidance**	27

Appendix 1 List of Authorised Officer Posts and Management Structure
Appendix 2 RIPA Flow Chart
Appendix 3 RIPA A Forms: Directed Surveillance
Appendix 4 RIPA B Forms: Covert Human Intelligence Source (CHIS) & Additional Notes
Appendix 5 Magistrates' Approval Process

The Regulation of Investigatory Powers Act 2000 ('RIPA') refers to 'Designated Officers'.
For ease of understanding and application within North Somerset Council, this Policy & Procedures Document refers to '**Authorised Officers'**. Furthermore, such Officers can only act under RIPA if they have been duly certified by the Head of Legal & Democratic Services. For the avoidance of doubt, therefore, all references to duly certified **Authorised Officers** refer to 'Designated Officers' under RIPA.

The terms 'he' and 'his' are used throughout this document when referring to an Authorised Officer and/or the subjects of surveillance. This is simply for ease of reference and does not indicate an assumption they are male.

A

Introduction, Key Messages and Why Surveillance is Necessary

1. This Policy & Procedures Document is based upon the requirements of The Regulation of Investigatory Powers Act 2000 ('RIPA') and Home Office's Code of Practices on Covert Surveillance and Covert Human Intelligence Sources.

2. The authoritative position on RIPA is 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 Deputy s151 Officer, for advice and assistance**.

   Appropriate training and development will be organised by the Deputy s151 Officer to relevant Authorised Officers and other senior managers.

3. Copies of this document and related Forms will be placed on the Council's Intranet or available from the Internal Audit Service.

4. The Internal Audit Service will maintain and check the Council's Register of all RIPA authorisations, review, renewal, cancellation and rejections on behalf of the Head of Legal & Democratic Services. It is the responsibility of the relevant Authorised Officer, however, to ensure the Internal Audit Service receives a copy of the relevant Forms within 1 week of authorisation, review, renewal, cancellation or rejection.

5. RIPA and this document are important for the effective and efficient operation of North Somerset Council's actions with regard to covert surveillance and the use of Covert Human Intelligence Sources (CHIS).

   This document will therefore, be kept under **annual** review by the Deputy s151 Officer. If any of the Home Office Codes of Practice or Forms change, this document will be amended to reflect the changes

   In addition, Authorised Officers must bring any suggestions for continuous improvement of this document to the attention of the Deputy s151 Officer at the earliest possible opportunity.

6. In terms of monitoring e-mails and internet usage, it is important to recognise the important interplay and overlaps with North Somerset Council's e-mail and internet policies and guidance, the Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000 and the Data Protection Act 1998 and its Codes of Practice.

   Where Direct Surveillance of a member of staff's e-mail is considered the investigation will be managed under Lawful Business Monitoring and the Council's e-mail and internet policies as surveillance is likely to be more relevant under the contract of employment terms as opposed to RIPA directed surveillance.

   In such cases, an Impact Assessment Form will be authorised in order to provide suitably justification for the action.

   RIPA forms will only be used where relevant and they will be only relevant where the Direct Surveillance relates to the lawful purpose available to local authorities.

7. **At no time should Council Officers carry out any surveillance that interferes with any private property.**
   Placing tracking devices on a subject's vehicle or person are <u>not authorised</u> for local authorities and must not be used.

8. **If you are in any doubt on RIPA, this document or the related legislative provisions, please consult the Deputy s151 Officer, for advice at the earliest possible opportunity.**

9. Why Surveillance is Necessary by Officers of North Somerset Council

In general, observation forms part of the duties of many enforcement officers and is not usually regulated by the RIPA 2000 Act. A **Trading Standards Officer** might covertly observe and then visit a shop as part of their enforcement function to verify the supply or level of supply of goods or services that may be liable to a restriction or tax.

Similarly, **Housing Benefit Investigators, Planning Officers and many other members of staff** within North Somerset Council may be required to carry out Directed Surveillance in order to establish information regarding an individual that they are unable to obtain through less intrusive means.

In addition, the provisions of RIPA do not normally cover the use of overt CCTV surveillance systems, as members of the public are aware that such systems are in use, however, there may be occasions when North Somerset Council use overt CCTV systems for the purposes of a specific investigation or operation. **In such cases, an authorisation for Directed Surveillance may be necessary.**

See Section G

RIPA provides that all codes of practice relating to the Act are admissible as evidence in criminal and civil proceedings and if any provision appears relevant to any court or tribunal, or to one of the Commissioners responsible for overseeing the powers conferred by the RIPA 2000 Act, it must be taken into account.

10. Grounds for Authorisation of Directed Surveillance and for the Use of Covert Human Intelligence Sources

The only lawful purpose available to the council is:

For the purpose of Preventing or Detecting crime as no other grounds are available to Local Authorities. Local authorities can no longer authorise directed surveillance for the purpose of preventing disorder, unless this involves a criminal offence(s) punishable by a maximum term of at least 6 months' imprisonment.

11. General Rules on Authorisation

An authorisation under Part II of the RIPA 2000 Act will provide **lawful** authority for a public authority to carry out surveillance.

Where there is an interference by a public authority with the right to respect for private and family life guaranteed under Article 8 of the European Convention on Human Rights, and where there is no other source of lawful authority, the consequence of not obtaining an authorisation under the RIPA 2000 Act may be that the action is unlawful by virtue of section 6 of the Human Rights Act 1998.

When you authorise surveillance against someone, you are effectively suspending their Human Rights.

Therefore, all authorisations MUST be cancelled immediately they are no longer required or when surveillance has ceased.

As such, North Somerset Council recommend officers seek an authorisation on each occasion where the surveillance is likely to interfere with a person's Article 8 rights to privacy by obtaining private information about that person, whether or not that person is the subject of the investigation or operation.

Obtaining an authorisation and Magistrates Court approval will ensure that the action is carried out in accordance with law and subject to stringent safeguards against abuse.

B

North Somerset Council Policy Statement

1. North Somerset Council takes seriously its statutory responsibilities and will, at all times, act in accordance with the law and take necessary and proportionate action in these types of matters.

In that regard, the Head of Legal & Democratic Services, 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 Head of Legal & Democratic Services is also authorised to add or substitute Officers authorised for the purpose of RIPA.

2. The Council's Executive resolved as follows:

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

(b) that only those Officers identified in Appendix 1 of this policy be permitted to authorise a covert surveillance exercise or use of a covert human intelligence source; and;

(c) that the policy and procedure be circulated to all Council Officers which may potentially carry out covert surveillance or obtain information from a covert human intelligence source (CHIS).

Inspection Process - Oversight by Commissioners

The Office of Surveillance Commissioners was set up in May 2001 to control surveillance activity by authorised public bodies.

The RIPA 2000 Act requires the Chief Surveillance Commissioner to keep under review (with the assistance of the Surveillance Commissioners and Assistant Surveillance Commissioners) the performance of functions under Part II of the RIPA 2000 Act by authorised public authorities and to provide independent oversight of the use of the powers contained within Part II of the RIPA 2000 Act.

North Somerset Council has had 4 inspection visits since 2001.

Inspections were carried out in September 2006, June 2008 and August 2012 and in the opinion of the Inspector, the Council's procedures for the application of the RIPA 2000 Act were operating to a good standard.

The last inspection, in August 2012 found the recent Policy and Procedures to be 'highly commended'.

It made several recommendations which include;

- ✓ Refresher Training to improve content of applications and authorisations;
- ✓ Future authorisations of CHIS should be given careful consideration and be compliant with CHIS Code of Practice;
- ✓ Establish a protocol with the Police for their use of the council's CCTV equipment for covert surveillance which reflects council policy and best practice.

The council accepted all the recommendations and has implemented them.

OSC Annual Reports also make recommendations which are countrywide and not specific to North Somerset Council.

C

Authorised Officer Responsibilities

1. It is essential, that Chief Officers and Authorised Officers in their Directorate, take personal responsibility for the effective and efficient operation of this Document.

The latest RIPA Forms used include the '5w's' (Who, what, why, when and where) approach to authorisation statements and each stage of the record history, i.e. application/review, renewal and cancellation forms are colour coded, thereby providing visual confirmation that the various record stages have been carried out.

2. The Head of Legal & Democratic Services has and will ensure that sufficient numbers of Authorised Officers from each Directorate are, after suitable training on RIPA and this Document, duly certified to take action under this Document.

3. The Council has a corporate responsibility to ensure that Authorised Officers are trained and duly certified and that Authorised Officers in turn must ensure that their relevant members of staff and enforcement officers are also suitably trained as 'Applicants' for RIPA authorisations to ensure applications are appropriate and well prepared..

4. Authorised Officers must acquaint themselves with the relevant Codes of Practice issued by the Home Office regarding RIPA as any failure to comply exposes North Somerset Council to unnecessary legal risks and criticism from the Office of Surveillance Commissioners.

Cancellations must be promptly dealt with.

5. Authorised Officers will also ensure that staff who report to them follow this Policy & Procedures Document and do not undertake or carry out any type of surveillance without first obtaining the relevant authorisations in compliance with this Document.

6. Authorised Officers must also pay particular attention to Health and Safety issues that may be identified as a result of any proposed surveillance activity.

Under no circumstances, should an Authorised 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. In regard to a CHIS application the risk assessment relating to the covert exercise must be provided and the Authorising Officer and used in their consideration of approving the application.

If an Authorised Officer is in any doubt, s/he should obtain prior guidance on the same from his/her Chief Officer, the Council's Health & Safety Officer and/or the Deputy s151 Officer.

Authorised Officers must also ensure that, when sending copies of any Forms to the Internal Audit Service that they are sent in **sealed** envelopes and marked '**Strictly Private & Confidential', to be opened by addressee only.**

7. Authorised Officer Considerations (see Item I5)

On receipt of an investigating officer's Application Form for Directed Surveillance or CHIS the Authorising Officer must re-evaluate the circumstances of the investigation with regard to **Necessity, Proportionality and Collateral Intrusion.**
The circumstances of each individual activity should be considered on its own merit as the legal principles applied to particular facts of covert surveillance is, ultimately, a matter of judgment.

8. Necessity and Proportionality (see also I-5(c))

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

9. Collateral Intrusion (see also I-5(f))

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

Surveillance Officers 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 reviewed, amended and either re-authorised or a fresh authorisation granted.

10. Retention and destruction of product of surveillance (see also I-12)

Where material obtained from the surveillance is considered 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.

Authorised Officers must ensure, therefore, that arrangements are in place for the handling, storage and destruction of material obtained through the use of covert surveillance.

Authorised 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.

11. Confidential Information (See also I-5(g))

Special safeguards apply with regard to confidential information relating to legal privilege, personal information and journalistic material. The Authorised Officer and the surveillance officer must understand that such information is confidential and can not be obtained.

Therefore, the risk of identifying confidential information during surveillance must be given prior consideration before an application is authorised. Failure to do so may invalidate the admissibility of any evidence obtained.

Consideration must also be given to the retention and disposal of any material obtained under a RIPA Authorisation before any forms are signed.

Where there is a likelihood of confidential information being obtained through covert surveillance, the application must be authorised by the Chief Executive, or in his absence, the Head of Legal and Democratic Services.

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

D

General Information on RIPA

A flowchart of the procedures to be followed for Directed Surveillance and CHIS is attached as Appendix 2.

1. The Human Rights Act 1998 requires North Somerset 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 correspondence.

2. The European Convention on Human Rights and Fundamental Freedom 1950 did not, however, make this an absolute right, but a qualified right. Accordingly, in certain circumstances, North Somerset Council may interfere in the citizen's right mentioned above, if such interference is:-

(a) **Lawful,** (in accordance with the law);
(b) **Necessary** (as defined in this Document); **and**
(c) **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 '**C**overt **H**uman **I**ntelligence **S**ource' **('CHIS')** - e.g. Informant.

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.

In certain circumstances, it permits Public Authorities to compel telecommunication and postal companies to obtain and release communications and data used by them using a Home Office trained **S**ingle **P**oint **o**f **C**ontact **(SPoC)**.

Authority to access this type of data will be subject to a separate North Somerset Council policy document.

4. Directly employed Council staff and external agencies working for North Somerset Council are covered by the Act for the time they are working for the Council.

All external agencies must, therefore, comply with RIPA; and;

When working on behalf of the Council in the capacity of carrying out covert activities or investigative work, external agencies must ensure that RIPA applications are properly authorised by one of the Council's designated Authorised Officers.

Authorised Officers are listed in Appendix 1 to this Document and, duly added to, or substituted by, the Head of Legal & Democratic Services.

5. If the correct procedures are not followed,

(a) the Courts may disallow evidence;
(b) a complaint of maladministration could be made to the Ombudsman, and/or
(c) the Council could be ordered to pay compensation.

Such action would not, of course, promote the good reputation of North Somerset 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 **Deputy s151 Officer**

E

What RIPA Does and Does Not Do

1. RIPA does:

(a) **require <u>prior authorisation</u>** of **<u>Directed Surveillance</u>**;

(b) **prohibit** the Council from carrying out **<u>Intrusive Surveillance;</u>**

(c) **require <u>authorisation</u>** of the conduct and use of a **<u>CHIS;</u>**

(d) **require <u>safeguards</u>** for the conduct and use of a **<u>CHIS;</u>**

(e) **<u>compels disclosure</u>** of communications data from telecommunications and postal service providers; *

(f) **<u>permits</u>** the Council to obtain communications records from Communication service providers. *

* (subject to a separate policy)

2. RIPA does not:

(a) allow unlawful conduct;

(b) prejudice or dis-apply any existing powers available to North Somerset 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 Authorised Officer or any Applicant is in any doubt, s/he should ask the Deputy s151 Officer <u>BEFORE</u> any Directed Surveillance and/or CHIS is authorised, renewed, cancelled or rejected.

F

Types of Surveillance

Section 26(2) RIPA does not differentiate between the gathering of current and historical data as a result of surveillance, therefore monitoring, research or analysis carried out now on past events or movements of an individual to establish a pattern or relationships is capable of being directed covert surveillance and an authorisation should be considered.

'Surveillance' includes

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

Surveillance can be Overt or Covert.

1. *Overt Surveillance*

Most of the surveillance carried out by North Somerset Council will be done overtly – there will be nothing secretive, clandestine or hidden about it.

In many cases, Officers will behave in the same way as a member of the public and/or will be going about Council business openly where they do not establish or maintain a relationship for the purpose of covertly obtaining information. (e.g. in the case of most test purchases or a market inspector walking through markets).

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; (See Section G and H 4.4(b)) 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.

2. *Covert Surveillance*

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

It cannot however, be authorised as "necessary" if there is a reasonably available overt means of obtaining the required information that has not yet been tried.

Notwithstanding this point, where the required information may feasibly be obtained in a less intrusive means but in so doing may jeopardise the outcome of the investigation, the surveillance can be authorised.

The applicant and subsequently the Authorising Officer, must provide a justifiable and sound reason for doing so and outline their reasons on the application.

RIPA regulates two types of covert surveillance,

- Directed Surveillance and Intrusive Surveillance and,
- the use of Covert Human Intelligence Sources **(CHIS).**

3. *Directed Surveillance*

Directed Surveillance is surveillance which:-

- is covert but not **intrusive** (See definition Item F6)

The Council **must not** carry out any **intrusive** surveillance or any **interference** with private property;

- is carried out 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 a subject for purposes of an investigation). (Section 26(10) of RIPA).
- is planned and not carried out in an immediate response to an event or circumstance, the nature of which could not have been foreseen and for which it would not have been practicable to seek an authorisation under the act, e.g. spotting something suspicious and continuing to observe it.

  However, in this case, consideration must always be given to whether an urgent authorisation must be required should the event or circumstance continue.

4. *Private information*

Private information in relation to a person includes any information relating to private and family life, home and correspondence. The fact that covert surveillance occurs in a public place or on business premises does not mean that it cannot result in the obtaining of private information about a person.

Prolonged surveillance targeted on a single person will undoubtedly result in the obtaining of private information about him/her and others that s/he comes into contact, or associates, with.

Similarly, 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.

For the avoidance of doubt, **only** those Officers designated and certified to be **'Authorised 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 Authorised 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 Policy & Procedures Document.

5. *Intrusive Surveillance*

This form of surveillance can only be carried out by the Police and other Law Enforcement Agencies – Intrusive Surveillance **Must Not** be carried out by Council Officers.

Intrusive surveillance is when it:-

- is covert;
- relates to residential premises and/or private vehicles; and;
- involves the presence of a person in the premises or in the vehicle or is carried out by a surveillance device in the premises/vehicle. Surveillance equipment mounted outside the premises will not be intrusive, unless the device consistently provides information of the same quality and detail as might be expected if they were in the premises/vehicle.

6. *Property Interference*

Any interference with property will require RIPA authorisation from the Police.

A Local Authority is not entitled to interfere with property for the purposes of surveillance.

7. ***Tracking Devices and Vehicle Tracking Devices***

In the event of there being a requirement for a vehicle tracking device to be used, and that to install/affix such a device, requires interference with property **not** owned by North Somerset Council, it is recommended that the RIPA authorisation from the Police is used.

Tracking devices placed in Council owned vehicles is unlikely to be classed as covert as the staff are aware that they are used for recording business movements.

If however, the device is to be used for a purpose not previously notified to the occupants an appropriate covert directed authorisation should be granted.

Any proposals for the use of Vehicle Tracking Devices need to be discussed with the **Deputy s151 Officer** so that a decision can be made on the matter in light of the circumstances in which the vehicle tracking device might be used.

8. ***Networking Sites (SNS)***

Care must be taken when authorising a request to access a SNS.

Whilst it is the responsibility of the individual to set their privacy settings it is unwise to regard it as 'open source' or publicly available as the individual has a reasonable expectation of privacy if access controls are in place.

It is not unlawful for a member of a public authority to set up a false identity but it is unadvisable to do so for a covert purpose without an authorisation. (See also H 4.5)

G

Examples of different types of Surveillance

Type of Surveillance	Examples
'Drive by'	'Drive by' surveillance may or may not need an authorisation, it is **not** acceptable to prescribe a minimum number of passes before an authorisation is required. OSC Procedures and Guidance 2011
Overt	▪ Police Officer or Parks Warden on patrol; ▪ Sign-posted 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 than a member of the public) (see F2)
Covert but not requiring authorisation	Recording of suspected noise nuisance where the intention is only to record excessive noise levels from adjoining premises and the device is calibrated as such. In such circumstances the perpetrator would normally be regarded as having 'forfeited' any claim for privacy.
Covert but not requiring prior authorisation	CCTV cameras providing general traffic, crime or public safety information.
Directed requiring RIPA authorisation	CCTV or ANPR (Automated Number Plate Recognition) when the system is targeted to record movements of a specific person or vehicle (ANPR) over a period of time or distance in order to monitor activity.
Covert e-trading	A CHIS authorisation is only required for the use of an internet trading organisation such as eBay when a covert relationship is likely to be formed. The use of 'disguised' purchaser details in a simple 'overt', electronic purchase does not require a CHIS authorisation, because no relationship is usually established at that stage. - OSC Procedures and Guidance 2011
Cover Networking Sites (SNS)	It is not unlawful for a member of a Local Authority to set up a false identity but it is unadvisable to do so for a covert purpose without an authorisation. (See also F8) A CHIS authorisation is only required when a covert relationship is likely to be formed.
Directed must be RIPA authorised. A ***CHIS*** 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 about the private life of a shop owner, e.g. where s/he is suspected of running a business in an unlawful manner. ▪ Where the officer or another person will be maintaining or establishing a covert relationship for a covert operation.
Intrusive	Planting a listening or other device (bug) or camera in a person's home or in/on their private vehicle/person. **North Somerset Council CANNOT carry out Intrusive Surveillance**

H

Conduct and Use of a Covert Human Intelligence Source (CHIS)
*** See also Appendix 4**

A Covert Human Intelligence Source (CHIS) may include those referred to as agents, informants and officers working undercover.

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

1. Covert Human Intelligence Source Code of Practice (COP) 2010 Definition

COP 2.1 Under section 26(8) of the 2000 Act a person is a source if:

(a) *he establishes or maintains a personal or other relationship with a person for the covert purpose of facilitating the doing of anything falling within paragraph (b) or (c);*

(b) *he covertly uses such a relationship to obtain information or to provide access to any information to another person; or*

(c) *he covertly discloses information obtained by the use of such a relationship or as a consequence of the existence of such a relationship.*

COP 2.2 By virtue of section 26(9)(b) of the 2000 Act – A relationship is established or maintained for a covert purpose if and only if it is conducted in a manner that is calculated to ensure that one of the parties to the relationship is unaware of the purpose.

COP 2.3 By virtue of section 26(9)(c) of the 2000 Act - A relationship is used covertly, and information obtained is disclosed covertly, if and only if the relationship is used or the information is disclosed in a manner that is calculated to ensure that one of the parties to the relationship is unaware of the use or disclosure in question.

2. Who is a CHIS?

- ✓ Someone who establishes and/or maintains a personal, or other relationship, for the covert purpose of helping the covert use of the relationship to obtain information.
- ✓ RIPA does not apply in circumstances where members of the public volunteer information to North Somerset Council as part of their normal civic duties, or to contact numbers set up to receive information.
- ✗ CHIS does not apply if someone is just tasked to do something without establishing a relationship.

3. What must be authorised?

- ✓ The **Conduct** or **Use** of a CHIS requires **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.
  - Maintenance of a **confidential record** of the CHIS which is held securely. (See Appendix 4)

4. When / When not to grant a CHIS - Examples

4.1 Juvenile Sources (see also H4.3)

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.

When a young person carries out a test purchase at a shop on a single occasion he is unlikely to be a CHIS, however, if more than one visit is carried out this would become a CHIS.

If covert recording equipment is worn an adult is observing the purchase a directed surveillance authorisation should be obtained.

Only the **Chief Executive Officer or (in his absence) the Head of Legal and Democratic Services are duly authorised to use Juvenile Sources**, as there are other onerous requirements for such matters.

Whilst a combined authorisation can be given for both a CHIS and Directed Surveillance the respective forms A1 and B1 must be completed and duly authorised.

4.2 Vulnerable Individuals

A Vulnerable Individual is described in the Act, as 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.

Only the **Chief Executive Officer or (in his absence) the Head of Legal and Democratic Services are duly authorised to use Juvenile Sources**, as there are other onerous requirements for such matters.

4.3 Test Purchases (see also H4.1)

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).

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.

Whilst a combined authorisation can be given for both a CHIS and Directed Surveillance the respective forms A1 and B1 must be completed and duly authorised.

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

(a) Persons who complain about anti-social behaviour, and are asked to keep a diary, will not normally be considered 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.

(b) Recording sound (with a DAT recorder) on private premises could constitute either directed or intrusive surveillance, dependent upon whether it is carried out overtly and upon the type of equipment used.

For example, it will be possible to carry out a recording if the noisemaker is warned that this will occur if the level of noise continues. However, the warning is not infinite and if a similar operation is instigated against the subject a further warning letter should be provided.

The surveillance may be deemed as intrusive if the recording equipment is so sensitive that it records personal information.

The Council should have in place a monitoring policy that clearly sets an early review of the recording by the Authorised Officer to determine whether surveillance should continue or be cancelled.

Placing a stationary or mobile video camera outside a building to record anti social behaviour on residential estates will require prior authorisation.

4.5 Covert e-trading

- ✓ A CHIS authorisation is only required for the use of an internet trading organisation such as eBay when a covert relationship is likely to be formed.
- ✓ The use of 'disguised' purchaser details in a simple 'overt', electronic purchase does not require a CHIS authorisation, because no relationship is usually established at that stage. - OSC Procedures and Guidance 2011

See also item F8

Further guidance on CHIS can be found in the Home Office's Code of Practice on Surveillance

I

Application and Authorised Officer considerations and Procedures

An Authorisation does not lapse or "time out"!

Each Authorisation MUST be Cancelled,

1. ***Directed Surveillance*** and the use of a CHIS can only be lawfully carried out if properly authorised, and in strict accordance with the terms of the authorisation.

   Appendix 2 provides a flow chart of process from application / consideration, to recording of information.

2. ***Authorised Officers***

   - Forms can only be signed by Authorised Officers listed in Appendix 1.

     This Appendix will be kept up to date by the Head of Legal & Democratic Services and added to as needs require.

     If a Chief Officer wishes to add, delete or substitute a post, s/he must refer such request to the Head of Legal & Democratic Services for consideration, as necessary.

     The Head of Legal & Democratic Services has been duly authorised to add, delete or substitute posts.
   - Authorisations under RIPA are separate from delegated authority to act under the Council's Scheme of Delegation and internal directorate Schemes of Delegation.
   - All RIPA authorisations are for specific investigations only, and **must** be reviewed, renewed or cancelled once the specific surveillance is complete or about to expire.
   - Authorised Officers must be mindful of potential 'self authorisations' where, due to the size of the Service and environment they work within may be a likely occurrence.

     Every effort should be made to ensure that Authorised Officers are not actively involved in, or have a 'working' knowledge of an operation where an application for an authorisation is requested.

3. ***Judicial Approval (SI 2012/15)***

   On 1 May 2012 the Protection of Freedoms Act 2012 became law and introduced a number of measures, including the amendment to the RIPA 2010 Order. Two provisions of the Act have particular relevance to covert surveillance investigations.

   a) Firstly, a new duty, from 1 November 2012, to obtain **Judicial approval** before exercising existing powers available under RIPA. In each case, the role of the Magistrate is to ensure that the correct procedures have been followed and the relevant factors have been taken into account. This is in addition to the authorisation by an Authorising Officer who meets the criteria regarding their position within the authority.

      Approval can only be given if the Magistrate is satisfied that:

      i. There were reasonable grounds for the authorising officer approving the application to believe that the Directed Surveillance or deployment of a CHIS was necessary and proportionate and that there remain reasonable grounds for believing so.

      ii. The authorising officer was of correct seniority within the organisation.

   See Appendix 5 – Magistrates' Approval Process

b) Secondly the Act, from 1 November 2012 introduces restrictions on the use of surveillance powers by Local Authorities, namely the can be used only for directed surveillance, where it is for the purpose of detecting or preventing a criminal offence and the offence is one that has a maximum sentence of at least six months imprisonment or would constitute and offence under sections 146, 147 or 147A of the Licensing Act 2003 or section 7 of the Children and Young Persons Act 1933. The latter are all offences involving sale of tobacco and alcohol to underage children.

4. *Grounds for Authorisation*

Directed Surveillance (A Forms) or the Conduct and Use of the CHIS (B Forms) can be authorised by North Somerset Council only on the grounds of **'preventing or detecting crime'** as no other grounds are available to Local Authorities. Local authorities can no longer authorise directed surveillance for the purpose of preventing disorder, unless this involves a criminal offence(s) punishable by a maximum term of at least 6 months' imprisonment.

The Applicant should state the relevant legislation, i.e. Theft Act, Sale of Copyright Designs and Patents Act 1988 etc;

The Authorising Officer must be satisfied that the conduct of covert surveillance explained, clearly identifies and describes as necessary and proportionate what it is aiming to prevent or detect with regard to the legislation, particularly if there is any doubt.

Any person applying for an authorisation will also need to be aware of particular sensitivities in the local community where the surveillance is taking place and of similar activities being carried out by other public authorities that could impact on the deployment of surveillance.

5. *Surveillance Request Forms (Application, Review, Renewal and Cancellation)*

Only the approved RIPA forms set out in this Document must be used and requested from the Internal Audit Service who will issue a Unique Reference Number (URN - **Year / Number of Application**) for the surveillance operation which will be recorded in the Central Register.

Any other forms used will be rejected by the Authorised Officer and/or the Deputy s151 Officer and/or Internal Audit Service.

A Forms	(Directed Surveillance) – See Appendix 3
Form A1 (White)	Application for Authority for Directed Surveillance
Form A2 (Yellow)	Review of Directed Surveillance Authority
Form A3 (Green)	Renewal of Directed Surveillance Authority
Form A4 (Pink/Red)	Cancellation of Directed Surveillance

B Forms	(CHIS) – See Appendix 4
Form B 1 (White)	Application for Authority for Conduct and Use of a CHIS
Form B 2 (Yellow)	Renewal of Conduct and Use of a CHIS
Form B 3 (Green)	Review of Conduct and Use of a CHIS
Form B 4 (Pink/Red)	Cancellation of Conduct and Use of a CHIS

6. *Assessing the Application Form for Authorisation - Form A1 (White)*

Before an Authorised Officer signs a Form, they must:-

(a) Be mindful of this Policy & Procedures Document, the Training provided and any other guidance issued, from time to time by Deputy s151 Officer on such matters,

and the recommendations made by the Office of Surveillance Commissioners Inspector.

(b) Be satisfied that the RIPA authorisation is:-

(i) **in accordance with the law for 'preventing or detecting crime'**
(ii) **necessary** in the circumstances of the particular case on one of the grounds mentioned in paragraph 3 above; and;
(iii) **proportionate** to what it seeks to achieve.

(c) **Necessity and Proportionality**

The Authorised Officer must ensure proper regard is had to necessity and proportionality before any applications are authorised. 'Stock phrases' or cut and paste narrative must be avoided at all times as the use of the same may suggest that insufficient detail had been given to the particular circumstances of any person likely to be the subject of the claim.

Any equipment to be used in any approved surveillance must also be properly controlled, recorded and maintained for audit purposes.

Authorising Officers must be careful in the use of "or" and "and" in order not to restrict what is intended. For example, do not use "or" when "and" is meant (e.g. "deployment of X on vehicle A or vehicle B" limits deployment to either vehicle, not both simultaneously or one after the other).

(d) Assess whether or not the proposed surveillance is **NECESSARY**

Ensure that the application accurately details and reflects the action taken so far and the proposed activity;

(e) Assess whether or not the proposed surveillance is **PROPORTIONATE** to the benefit of the potential outcome.

Firstly consider if:

- the proposed covert surveillance is proportional to the mischief under consideration;
- it is proportional to the degree of the anticipated intrusion on the targets and others;
- it is the only option, other over means having been considered and discounted.
- also consider other appropriate means of gathering the information;
- consider the number of officers to be used and the period of surveillance;
- consider what equipment is requested to be used;
- how intrusive might it be on the subject of surveillance or on others? And;
- why is this intrusion outweighed by the need for surveillance in operational terms or can the evidence be obtained by any other means? [Code paragraph 3.4]

All this is relevant as the least intrusive method will be considered proportionate by the courts.

A comment such as "I authorise the activity as stated" is insufficient.

It must be explained why this Directed Surveillance is proportionate to what it seeks to achieve. (See note below - Statutory Instrument 2012 No. 1500)

Statutory Instrument 2012 No.1500

The Statutory Instrument makes an amendment to the RIPA 2000 Act in that it sets conditions under which surveillance powers should and should not be considered.

The amendments were laid before parliament on the 14th June 2012 and come into force with effect from1st November 2012.

Local Authorities must **not** use their Surveillance powers to tackle dog fouling littering offences, snooping on the contents of families' bins and security checking school-run parents as they are not considered necessary for public safety.

From 1 Nov 2012, Local Authorities face severe restrictions on the grounds for which they can authorise Directed Surveillance under RIPA.

Authorising Officers may **not** grant authorisation to carry out of Directed Surveillance unless it is for the purpose of preventing or detecting a criminal offence and meets the condition set out in new article 7A (3) (a) or (b).

Those conditions are; that the criminal offence which is sought to be prevented or detected is punishable, whether on summary conviction or on indictment, by a maximum term of at least 6 months of imprisonment, or would constitute an offence under sections 146, 147 or 147A of the Licensing Act 2003 or section 7 of the Children and Young Persons Act 1933.

(f) Collateral Intrusion

In addition, before authorising surveillance for necessity and proportionality, the Authorised Officer should take into account the risk of intrusion into the privacy of persons other than the directly the specified subject(s) of the surveillance, investigation or operation.

Measures must be taken, wherever practicable, to avoid or minimise (so far as is possible) unnecessary **Collateral Intrusion** into the lives of those not directly connected with the investigation.

Officers carrying out the surveillance should inform the Authorised 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 reviewed, amended and either re-authorised or a fresh authorisation granted.

Any person granting an authorisation will also need to be aware of particular sensitivities in the local community where the surveillance is taking place and of similar activities being carried out by other public authorities that could impact on the deployment of surveillance.

(g) Confidential Information

Consider authorisations that involve **Confidential Information** as special safeguards apply with regard to confidential information. The RIPA 2000 Act does not provide any special protection for ‘Confidential Information’.

Nevertheless, particular care should be taken in cases where the subject of the investigation or operation might reasonably expect a high degree of privacy, or where confidential information is involved.

Confidential information consists of;

(a) Matters subject to Legal Privilege; as defined in the Police Act 1997 (PA), s98 (communications between a professional legal adviser and his client or representative);

(b) Confidential Personal Information as defined under PA s99, personal information acquired by trade, business or profession, information held relating to the spiritual, physical or mental health of an individual (whether living or

dead) who can be identified from it, such as consultations between a health professional and a patient, or; information from a patient's medical records;

(c) Confidential Journalistic Material; PA s100 - material acquired or created for the purposes of journalism; and;

(d) Confidential constituency information;

The Authorised Officer and the surveillance officer must understand that such information is confidential and cannot be obtained.

Therefore, the risk of identifying confidential information during surveillance must be given prior consideration before an application is authorised. Failure to do so may invalidate the admissibility of any evidence obtained.

Consideration must also be given to the retention and disposal of any material obtained under a RIPA Authorisation before any forms are signed.

In cases where, through the use of surveillance, it is likely that knowledge of confidential information will be acquired, the use of surveillance is subject to a higher level of authorisation.

Such authorisation can only be provided by the Head of Paid Service (Chief Executive Officer) or (in their absence) a Chief Officer.

Appendix 1 lists the authorising officer permitted to authorise such surveillance.

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

(h) Duration of Authorisation and frequency of reviews

- ✓ Initial Authorisations will last for 3 months and should not be authorised for any period less;

  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 and MUST be cancelled.**
- ✓ Authorise **only** if an overt or less intrusive option is not practicable.

  If a less intrusive option has not yet been attempted and is practicable the application must be **rejected** and the reason stated in the relevant comments box.

  The Courts will consider the least intrusive method of investigation.

(i) Review dates

- ✓ Authorised Officers must set realistic review dates at intervals of no longer than **1 month or 28 days** after the date of initial authorisation; and less if there is a change in circumstance. If it is over a month it may be difficult to demonstrate effective management of the activity and setting a review date of 3 months could be considered unjustifiable.
- ✓ Authorised Officers must set an appropriate date for **review** of the authorisation and review should be carried out only on that date,
- ✓ The review periods are decided by the Authorising Officer based on the circumstances detailed in the application; and how long the applicant considers the activity is likely to take place.

(j) Central Register Update

Advise the Internal Audit Service of the authorised (**or** rejected) application in order that authorisation and review dates can be entered and relevant details recorded in the Central Register;
Ensure that any RIPA Directorate Register is duly completed.

(k) Form distribution and retention

The Original authorised (or rejected) RIPA Application Form (and any review/cancellation of the same) must be forwarded to the Internal Audit Service, **within 1 week** of the relevant authorisation, review, renewal, cancellation **or** rejection.

A copy of the authorised RIPA Application Form (and any review/cancellation of the same) must be held on the investigating officer's file in order for them to understand the parameters of the surveillance and equipment they have been authorised to carry out and use.

7. *Additional Safeguards when Authorising a CHIS - Form B1 (White)*

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

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

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

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

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

(e) Ensure records contain particulars and are not available except on a need to know basis;

(f) The 'authorisation' to carry out/conduct the CHIS lasts for a maximum **12 months** (from authorisation) for an **adult** and **1 month** for **Juvenile CHIS.** Whether the CHIS is used or not, in the relevant period, does not mean the 'authorisation' is 'spent', **the Forms do not expire and MUST be cancelled.**

The magistrate must be satisfied that:-

(g) The provisions of section 29(5) have been complied with. This requires North Somerset Council to ensure that there are officers in place to carry out roles relating to the handling and management of the CHIS as well as the keeping of records;

(h) Where the CHIS is under 18 years of age, the requirement of the RIPA (Juveniles) Order 2000 (SI 2000/2793) have been satisfied. This sets out rules about parental consent, meetings, risk assessments and the duration of the authorisation. Note that the authorisation of such person to act as a CHIS must come from the Chief Executive;

(i) Where the application is for the renewal of a CHIS authorisation, a review has been carried out by North Somerset Council and the magistrate has considered the results of the review.

8. *Urgent Authorisations*

(a) Urgent authorisations should not be necessary.

(b) However, in exceptional circumstances, an urgent authorisation may be given verbally (but only by an Authorising Officer) if the time that would elapse before a written authorisation can be granted would be likely to endanger life or jeopardise the investigation/operation to which the authorisation was sought.

(c) The Officer making the request must notate their records with details of authorisation.

(d) It will not be urgent where the need for authorisation has been neglected or is of the Officer's own making.

(e) **Urgent authorisations last for no more than 72 hours and all Forms must be completed.**

They must be recorded in writing on the standard Form A1 as soon as practicable and the extra boxes on the form completed to explain why the authorisation was urgent and forwarded to the Authorising Officer who granted verbal authority.

(f) If surveillance is to continue, complete Form A1 to cover verbal authorisation and renewal of surveillance.

(g) An Urgent Oral Authorisation, if not already ratified in a written authorisation, will cease to have effect after **72 hours**, beginning with the time when the authorisation was granted.

(h) If surveillance is to cease, complete Form A1 and Form A4 Cancellation together.

(i) Magistrates Court approval will still be required before the authorisation takes effect.

9. *Reviewing an Authorisation - Form A2 (Yellow)*

(a) All Applications (A1 Forms) **MUST** be reviewed by using the Form A2**.**

Frequent reviews of the operation should be carried out.

Reviews should be carried out, at least monthly or within the time stated on the set date (at least 28 days) (see Item I 5 I); or when there is a change in circumstance; so long as they are consistent with the terms of the original authorisation.

Changes may be;

- To add/remove a subject from the Authorisation.
- 'Unknown' subject becomes 'known'.
- To notify a new location.
- Changes to number of Officers.
- Changes to Collateral Intrusion

(b) The review process should be considered at least 3 days before the end date of the authorisation or review date in order for it to be far enough in advance but not so far that it may be affected by a potential change in circumstance.

An authorisation can be cancelled at any time before the due date of expiry.

(c) The Authorising Officer and Investigator should discuss the case under review and include;

- ✓ A summary of the events so far,
- ✓ The number of days on which surveillance has been carried out,
- ✓ What the surveillance has achieved to date? Is this what was sought on the original application? If not, why not?
- ✓ Update objectives and plan of action.

(d) If **accepted**, the Authorising Officer will return the Form A2 to the Investigator with comments;

(e) If **rejected,** the Authorising Officer must contact the Investigator to explain why and return the completed Form A2;

(f) Surveillance will **cease** from the time decided by the Authorising Officer.

(g) A **Cancellation Form A4** must be completed by the Investigator to formally cancel the surveillance operation.

10. *Renewing an Authorisation*

(a) Authorisations can be renewed in writing **no earlier than 5 days** before the end date of the initial authorisation. (Note: authorisations cannot 'expire' but must be cancelled).

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.

(b) The renewal will begin on the day when the authorisation would have been cancelled. In exceptional and urgent circumstances, renewals may be granted verbally and last for a period of **72 hours**.

(c) An Authorisation cannot be renewed after it has expired. In such an event a fresh Authorisation must be requested.

(d) Magistrates Court approval is required before a renewal takes effect.

11. ***Cancellation of an Authorisation - Form A4 (Pink/Red)***

(a) **Compare** what you have now with what you had before the surveillance commenced. * What have you achieved? * What haven't you achieved?

(b) **Remember**:

- Authorisations do not expire, they **MUST be cancelled immediately** they are no longer required and surveillance has ceased;
- Cancellation can be authorised **at any time,** you do not have to wait until the due expiry date has been reached;
- The investigator must complete the date and time of the last observations (box 1) and also include details of the total hours of surveillance carried out over the number of days.
- The investigator, should, where known, record the sanction applied as a result of the activity i.e. caution, admin penalty, conviction etc;

12. ***Training Records***

- Appropriate training will be given (or approved) to applicants and Authorised Officers.
- Before Authorised Officers are certified to sign any RIPA Forms they must have received training and be duly certified by the Head of Legal & Democratic Services.
- If the Head of Legal & Democratic Services feels that an Authorised Officer has not complied fully with the requirements of this Document, or the training provided, the Head of Legal & Democratic Services is duly authorised to retract that Officer's authorisation until s/he has undergone further approved training or a one-to-one meeting with the Head of Legal & Democratic Services.
- A central record of all officers and Authorised Officers who have received training or one-to-one meetings will be maintained by the Internal Audit Service.

13. ***Product of surveillance***

General Principles

Material obtained through covert surveillance **can** be used as evidence **provided that proper authorisation was given and the evidential trail has been preserved**

If material has been obtained incorrectly it cannot be used;

An Authorisation should be of a quality to withstand examination at trial or legal challenge;

In order to give proper consideration, the Investigating Officer and Authorising Officer should understand the capability of equipment, sensitivity levels of technical equipment intended to be used, and where and how it is to be deployed;

In addition, certain information may be obtained or automatically extracted than cannot be justified as necessary or proportionate giving rise to collateral intrusion.

If data is obtained outside the parameters of the authorisation, the AO should immediately review and arrange disposal.

Retention and destruction

Where material obtained from the surveillance is considered 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.

Authorised Officers must ensure, therefore, that arrangements are in place for the handling, storage and destruction of material obtained through the use of covert surveillance.

Authorised 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.

J

Working With / Through Other Agencies

1. When some other agency has been instructed on behalf of North Somerset Council to carry out 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 explicitly aware of what they are authorised to do.

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

(a) wish to use North Somerset 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 documentation sufficient documentary evidence from the requesting agency to provide an audit trail and to understand the parameters under which surveillance has been authorised.

You may only do what the Authorised Officer has authorised you to do on the application form.

A copy **and/or** relevant extracts of that agency's RIPA form should be requested for the record (a copy of which must be passed to the Internal Audit Service for the Central Register to demonstrate that the activity has been duly authorised) sufficient for the purposes of protecting North Somerset Council and the use of its resources ***1**

(b) wish to use the North Somerset 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 North Somerset 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.

***1** In terms of 2(a)
If the Police or other Agency wish to use North Somerset Council's resources for general surveillance (as opposed to specific RIPA operations) an appropriate Authorisation must be obtained before any Council resources are made available.

The authorisation should request;

- the proposed use,
- extent of remit,
- duration,
- who will be undertaking the general surveillance and,
- the purpose.

Consideration should be given to having a standard form for such instances that must be signed by the requesting agency.

If in doubt, please consult with the Deputy s151 Officer at the earliest opportunity.

K

Record Management

North Somerset Council Directorates must keep a detailed record of all authorisations, Magistrates approvals, renewals, cancellations and rejections.

In addition, a Central Register of all Authorisation Forms will be maintained and monitored by the Internal Audit Service, on behalf of the Head of Legal & Democratic Services.

Records to be maintained in the Directorate

For such purposes the relevant Chief Officer (or his/her designated Directorate Co-ordinator) must retain the following documents:

- a signed original of the Form(s) 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 signed original 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 Unique Reference Number (URN) for the authorisation or Rejection.

Each form will have a URN provided by the Internal Audit Service from the Central Register.

The Directorate Co-ordinator will advise the Applicant of the relevant URN for their case.

The cross-referencing of each URN takes place within the Forms for audit purposes.

Rejected Forms will also have URN's and the original copy of the rejected Form must be forwarded to the Internal Audit Service for completeness.

Central Register to be maintained by the Internal Audit Service

A Central Record of all application requests, authorised or rejected must be maintained, containing:

- URN; Unique Reference Number;
- The type of authorisation; Directed Surveillance or CHIS;
- The date authorisation was given; or rejected;
- Name/rank/grade of Authorising Officer;
- Title of the investigation and brief description/names;
- Urgency provisions used – if so, why;
- Whether or not the investigation is likely to result in obtaining confidential information;
- Whether the authorisation is a 'self authorisation';
- Review dates and dates when reviewed and If renewed, when and by whom;
- The date authorisation was **cancelled;**
- Outcome (value) of surveillance.

Authorised Officers must forward the signed original of the relevant form with all details, to the Internal Audit Service for the Central Register, within 1 week of the authorisation, review, renewal, cancellation or rejection.

The Deputy s151 Officer will monitor the same and give appropriate guidance, from time to time, or amend this document, as necessary.

North Somerset Council will retain ALL records for a period of at least **three** years from the date of CANCELLATION of the authorisation.

L

Implications for North Somerset Council for Non-compliance

Unless there are policies developed and introduced across North Somerset Council, how can managers be certain that surveillance activity occurs in compliance with RIPA?

This Policy document provides a framework within which all staff can comply with the legislation, and what, when and how to do it.

Investigating Enforcement Officers need to have as a minimum, an understanding of the legislation, to avoid and/or undue delay manifesting from avoidance.

Authorising Officers need to know and understand the requirement of the legislation, the necessity and proportionality of the activity, as well as knowing that cancellation is required as soon as the authorisation is no longer required.

Implications

Failure to correctly comply with the RIPA 2000 Act and procedures and guidelines results in the following implications;

To the Council

- If the evidence obtained is not lawfully authorised or implemented correctly within the parameters set, the evidence obtained may be excluded from court proceedings and costs ordered against the Council;
- The Council may have to pay compensation to the defendant and is no longer protected by section 27 RIPA2000; (*challenges to both the gathering of, and the subsequent use of, covertly obtained information*)
- RIPA powers could be withdrawn.

To the Authorising Officer

- The serious crime test is defined as an offence which carries a custodial sentence of six months or more.

To the individual

- The legal remedy provided by RIPA 2000 if a public body e.g. the Council breaches a persons Human rights, is to award compensation

The Law states that:

The Office of the Surveillance Commissioners (OSC) can, at any time, audit/review North Somerset Council's policies and procedures, and individual authorisations. If they are found to be unsatisfactory, authorisation for the Council to use surveillance may be withdrawn.

M

Concluding Guidance

1. Surveillance should not be carried out where there is;

(a) an interference with the right of respect for private life and family, guaranteed under Article 8 of the European Convention on Human Rights, and,

(b) where there is no other source of lawful authority for the interference, or;

(c) if it is considered 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 deemed unlawful by the Courts pursuant to Section 6 of the Human Rights Act 1998.

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 a person's human rights.

2. Authorised 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 North Somerset Council's responsibilities.

In order to evidence that the request has been correctly reviewed and understood, Authorised Officers must always complete, in handwriting, the "Authorising Officer's comments" box indicating the reason why authorisation is accepted.

The Authorising Officer must read and consider the Forms in full; and if authorising should;

- ✓ in their own words, describe and specify what they are granting, against which subjects, property or location and what equipment is to be used; This may or may not be the same as requested by the applicant;
- ✓ why they are satisfied/why they believe the activity is necessary, proportionate and manages any potential collateral intrusion; ("I am satisfied" and "I believe");
- ✓ Clearly write comments to demonstrate their reasons/thought process and understanding of the application in these areas; by explaining;

  "Who; What; Why; Where; When and How"

In order to demonstrate that due consideration has been applied to the application and authorisation process, **the use of 'template entries' should be avoided** or used with great care

3. 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.

The completion of Box 17 (Box 19 on the CHIS) is only necessary where confidential information or the urgency criteria is met.

4. Great care must also be taken to ensure accurate information is used and is inserted in the correct boxes.

5. Reasons for any refusal of an application must also be kept on the form and the form retained for future audits.

6. For further advice and assistance on RIPA, please contact the Deputy s151 Officer who will co-ordinate all Questions and Answers to the Office of Surveillance Commissioners and will act as the main contact person.