Appendix 1

COVERT SURVEILLANCE - REGULATION OF INVESTIGATORY POWERS ACT 2000 (RIPA) UPDATE

DONCASTER METROPOLITAN BOROUGH COUNCIL

Authorisation Procedures for the use of Directed Covert Surveillance and a Covert Human Intelligence Source (CHIS)

(In Compliance with Regulation of Investigatory Powers Act 2000)

1. Background

1.1 The use of surveillance to provide information is a valuable resource for the protection of the public and the maintenance of law and order. In order that local authorities and law enforcement agencies are able to discharge their responsibilities, use is made of surveillance and surveillance devices.

1.2 Where this surveillance is **planned** i.e. *is pre-meditated*, **and is covert**, i.e. *the subject of the surveillance is unaware that it is taking place*, then it must be authorised to ensure that it is lawful in accordance with the requirements of the **Regulation of Investigatory Powers Act 2000** ***(RIPA).***

1.3 **C.C.T.V.** systems in the main will not be subject to this procedure as they are 'overt' forms of surveillance. However, where **C.C.T.V.** is used as part of a pre-planned operation of surveillance then authorisation should be obtained.

1.4 From October 2000 planned Covert Surveillance became the subject of a legal framework to ensure that the use of surveillance is subject to **Senior Officer** authorisation, review and cancellation and that there is a procedure to support this.

1.5 In terms of monitoring e-mails and internet usage, it is important to recognise the important interplay and overlaps with the existing **DMBC** policy relating to e-mail and internet and guidance and also **The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000, The Data Protection Act 1987 and its Code of Practice.** Official ***RIPA*** forms should be used where **relevant** and they will be only **relevant** where the **criteria** listed on the Forms are fully complied with.

1.6 If you are in any doubt about the need to adhere to any ***RIPA*** related provisions or matters referred to in this document or the related legislative provisions, please consult the **Assistant Director Legal and Democratic Services (or Delegated Officer**), at the earliest possible opportunity.

1.7 At present Authorising Officers who can authorise surveillance are available in the following departments:

Legal
Revenue and Benefits
Trading Standards

2. Objective of This Procedure

2.1 The objective of this procedure is to ensure that all work involving Directed Surveillance by **D.M.B.C.** employees is carried out effectively, while remaining in accordance with the law and in particular does not breach **The Human Rights Act 1998.**

2.2 This procedure should be read in conjunction with the **Regulation of Investigatory Powers Act 2000** and the latest version of the **Codes of Practice** relating to the Use *of Covert Human Intelligence Sources* and *Directed Surveillance*, which is obtainable on the intranet website under 'Legal Services' or directly from the Assistant Director Legal and Democratic Services.

The Codes of Practice should be available to and read by all persons involved in completing applications and authorising *RIPA*-governed surveillance and information gathering.

PLEASE NOTE THIS IS THE MOST IMPORTANT DOCUMENT IN THE WHOLE *RIPA* RELATED PROCESS. YOU SHOULD FAMILIARISE YOURSELF WITH ITS CONTENTS AND STRICTLY FOLLOW THE PROCEDURES REFERRED TO SO THAT POTENTIALY SERIOUS LEGAL CONSEQUENCES ARE AVOIDED.

The Office of Surveillance Commissioners Procedures and Guidance is a useful document, available on the intranet and should be read in conjunction with the DMBC procedure.

3. Definitions

3.1 '**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

3.2 **Overt Surveillance**

Most of the surveillance carried out by the **DMBC** 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).

Similarly, surveillance will be Overt if the subject has been told it will happen (e.g. where an alleged noise nuisance 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).

3.3 **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*).**

RIPA regulates two types of Covert Surveillance.

(a) **Directed and Intrusive Surveillance**

(b) The use of **Covert Human Intelligence Sources *(CHIS).***

3.4 **Directed Surveillance**

Directed Surveillance is surveillance which:-

- is Covert; and

- is not **Intrusive Surveillance** (see definition below)

- **PLEASE NOTE, DMBC MUST NOT CARRY OUT INTRUSIVE SURVEILLANCE ;**

- is not carried out as an immediate response to events which would otherwise make seeking authorisation under the Act unreasonable, e.g. spotting something suspicious and continuing to observe it; **and**

- it is undertaken for the purpose of a specific investigation or operation in a manner likely to obtain private information about an individual (whether or not that person is specifically targeted for purposes of an investigation). (**Section 26(1) of *RIPA***).

Private Information in relation to a person includes any information relating to his private and family life, his home and his correspondence. The fact that Covert Surveillance occurs in a public place or on business premises does not mean that it cannot result in the obtaining of private information about a person. Prolonged surveillance targeted on a single person will undoubtedly result in the obtaining of private information about him/her and others that she/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'.

PLEASE NOTE THAT IT IS IMPERATIVE THAT DOCUMENTED PROCEDURES ARE FOLLOWED TO AVOID ADVERSE LEGAL CONSEQUENCES FOR PROCEDURAL FAILURES UNDER *RIPA*

The ***RIPA*** authorisation procedures detailed in this Document **MUST** be followed. If an Authorised Officer has not been '**certified**' for the purposes of ***RIPA***, he/she **CANNOT** carry out or approve/reject any action set out in this Document.

The surveillance of an employee relating to a disciplinary matter where the Council is looking to enforce its employment contract does not

usually fall within ***RIPA*** **(C v The Police and the Secretary of State for the Home Department (14th November 2006, No: IPT/03/32/H).** However any surveillance must ensure that it does not breach the right of an individual under **Article 8 of the HUMAN RIGHTS ACT 1998** and must also be proportionate and necessary.

The Information Commissioner's Officer has issued Employment Practice Codes (Part 3) which covers legal requirements this area.

3.5 **Intrusive Surveillance**

This is surveillance which:-

- 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 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.

This form of surveillance can be carried out only by police and other law enforcement agencies. **Council Officers MUST NOT carry out Intrusive Surveillance.**

3.6. Authorising Officer is the person who is entitled to give an authorisation for directed surveillance in accordance with the **Regulation of Investigatory Powers Act 2000.**

3.7 Private information includes information about a person relating to his private or family life.

3.8 Residential premises means any premises occupied or used, however temporarily, for residential purposes or otherwise as living accommodation.

3.9 Private vehicle means any vehicle that is used primarily for the private purpose of the person who owns it or of a person otherwise having the right to use it. (This does not include a person whose right to use a vehicle derives only from his having paid, or undertaken to pay, for the use of the vehicle and its driver for a particular journey.) A vehicle includes any vessel or aircraft. (For information vehicle tracking is overt)

3.10 ***CHIS (Covert Human Intelligence Source)*** is where the Council use someone to establish or maintain a personal or other relationship for the covert purpose of obtaining or passing on information.

4. PROCEDURE RELATING TO DIRECTED SURVEILLANCE or *CHIS*

4.1 This procedure applies in all cases where **'Directed Surveillance'** or ***'CHIS***' is being planned or carried out. Directed Surveillance is defined in the Code of Practice as surveillance undertaken "**for the purposes of a specific investigation or operation**" and "**in such a manner as is likely to result in the obtaining of private information about a person**".

4.2 The procedure **does not apply** to:

- **ad-hoc covert observations** that do not involve the systematic surveillance of specific person(s);
- **observations that are not carried out covertly**; or
- **unplanned observations made as an immediate response to events.**

Examples of different types of Surveillance

Type of Surveillance	Examples
Overt	- Police Officer or Parks Warden on patrol - Signposted Town Centre **CCTV** cameras (in normal use) - Recording noise coming from outside the premises after the occupier has been warned that this will occur if the noise persists. - Most **test purchases** (where the officer behaves no differently from a normal member of the public).
Covert but **not** requiring **prior** authorisation.	- **CCTV** cameras providing general traffic, crime or public safety information.
Directed **MUST** be ***RIPA*** authorised.	- Officers follow an individual or individuals over a period, to establish whether he/she is working when claiming benefit.
Intrusive **DMBC – PROHIBITED ACTIVITY**	- Planting a listening or other device (bug) in the home or in the private vehicle of a surveillance target.

5. EFFECT OF *RIPA* LEGISLATION

5.1 ***RIPA***

- **requires** Prior Authorisation of Directed Surveillance.
- **prohibits** the Council from carrying out **Intrusive Surveillance**.
- **requires** Prior Authorisation of the conduct and use of a ***CHIS***.
- requires safeguards for the conduct and use of a ***CHIS***.

5.2 ***RIPA* does not:**

- make unlawful conduct which is otherwise lawful.

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

5.3 If an **Authorised Officer** or any **Applicant** is in any doubt about any procedural obligations,he/she should ask the Head of Legal Services **BEFORE** any Directed Surveillance and/or a ***CHIS*** is authorised, renewed, cancelled or rejected.

6. Principles of Surveillance

6.1 In planning and carrying out Covert Surveillance, **D.M.B.C.** employees **MUST** adhere to the following principles:

6.2 **Lawful Purposes**

Directed Surveillance by a Local Authority shall only be carried out where necessary for the purpose of preventing or detecting crime, where the criminal offence sought to be prevented or detected is punishable by a maximum term of at least 6 months of imprisonment or are offences involving sale of tobacco and alcohol to underage children

Prior to 2004 Local Authorities did have other grounds for authorising surveillance but these have now been removed **(The Regulation of Investigatory Powers (Directed Surveillance and Covert Human Intelligence Sources) Order 2003.)** Prior to 1st November 2012 offences carrying less than 6 months imprisonment were able to be subject to covert surveillance but this has been restricted by the **Regulation of Investigatory Powers (Directed Surveillance and Covert Human Intelligence Sources) (Amendment) Order 2012.**

6.3 **Confidential Material**

Any Application which has been identified as containing a significant risk of acquiring confidential material **MUST** always **be authorised** by the **Chief Executive** or their **Deputy in their absence.**

6.4 For this purpose '**Confidential Material**' consists of: -

- **matters** subject to **legal privilege** (for example between professional legal advisor and client);

- **confidential personal information** (for example relating to a person's physical or mental health); or

- **confidential journalistic material**.

INTRUSIVE SURVEILLANCE

6.5 **A LOCAL AUTHORITY IS NOT PERMITTED TO CARRY OUT INTRUSIVE SURVEILLANCE**

6.6 Surveillance becomes Intrusive if the Covert Surveillance is carried out in relation to anything taking place on any **residential premises** or in any **private vehicle AND** involves the **presence of the person** undertaking the surveillance **on the premises or in the vehicle** of the subject of the surveillance **or** is carried out by means of a surveillance device which consistently provides information of the same quality and detail as might be expected to be obtained from a device actually present on the premises or in the vehicle.

DIRECTED SURVEILLANCE

7. AUTHORISATION PROCESS FOR DIRECTED SURVEILLANCE.

7.1 Directed Surveillance can only be lawfully carried out if **properly authorised** and in strict accordance with the terms of the authorisation. The form must be signed by an Authorising Officer and approved by a Magistrate before the authorisation can be acted upon.

7.2 **Authorised Officers and Magistrates Approval.**

A Central List of Authorised Officers will be retained by the Head of Legal Services. This should be kept up-to-date using the notification procedure. All Authorising Officers should have received adequate training on ***RIPA***.

7.3 Authorising Officers within the meaning of this procedure should avoid authorising their own activities. If this occurs it must be recorded on the pro forma sent with the Authorisation to Head of Legal Services on Directed Surveillance.

7.4 Once the form is signed by an Authorising Officer the Magistrates Court should be contacted to arrange for the application to be approved by a Magistrate.

7.5 **Application Forms**

All applications for Directed Surveillance Authorisations will be made on official designated stationery, which accords with the Code of Practice available on the intranet and **MUST** be personally completed by the applicant in all circumstances.

PERIOD OF VALIDITY OF AUTHORISATIONS

7.6 The Authorisation must be renewed in the time stated and cancelled once it is no longer needed. The Authorisation to conduct the Surveillance lasts for a maximum of 3 months for Directed Surveillance.

7.7 At the end of 3 months, if the need for the information continues and this is deemed to be the only way that it can be obtained, the original authorisation can be renewed. This is a prescribed process under the ***RIPA*** **Code of Practice.**

7.8 All applications for the renewal of Directed Surveillance must be made on the renewal form. The applicant in all cases should complete this where the surveillance is still required beyond the previously authorised period (including previous renewals).

7.9 Where authorisation ceases to be either necessary, appropriate or proportionate, the Authorising Officer **MUST** cancel an authorisation, using the cancellation form.

7.10 **All authorisations** must be reviewed <u>at least every 4 weeks from the date of authorisation,</u> using the renewal form, which must be attached to the original authorisation.

7.11 The respective forms, Code of Practice and supplementary material is available on the Council Intranet, or directly from Legal Services.

7.12 Services wishing to adopt a more devolved authorisation process may do so only on the explicit approval of a written policy by the Council; All authorisations must remain within the scope of the Code of Practice relating to persons permitted to authorise the activity required.

8. <u>Authorisation Criteria for Directed Surveillance</u>

8.1 Prior to granting an authorisation for the use of surveillance, the authorising officer must be satisfied that:-

- the authorisation is for a prescribed **lawful purpose (i.e. the prevention or detection of crime) where the criminal offence**

sought to be prevented or detected is punishable by a maximum term of at least 6 months of imprisonment or are offences involving sale of tobacco and alcohol to underage children;

- the purpose of the surveillance is clearly defined and stated.

- That any evidence obtained will be used if it relates to a specific section of specified Legislation appropriately identified and documented.

- account has been taken of the likely degree of intrusion into the privacy of persons other than those directly implicated in the operation or investigation (called **'Collateral Intrusion'**). Measures must be taken, wherever practicable, to avoid unnecessary intrusion into the lives of those affected by Collateral Intrusion. These measures and extent of possible intrusion should be recorded on the form;

- the authorisation is **necessary**;

- the authorised surveillance action is **proportionate** to the information being sought;

- any **equipment** to be used is **specified**;

- the information required **cannot be obtained by alternative methods.**

8.2 **Necessity**

Surveillance operations shall only be undertaken where there is no reasonable and effective alternative way of achieving the desired objective(s) for the purpose of preventing and detecting crime, preventing disorder and the use of Directed Surveillance is the most reasonable means of obtaining the evidence or intelligence to support a prosecution.

8.3 **Effectiveness**

Surveillance operations shall be undertaken only by **suitably trained or experienced employees**, or under their direct supervision.

8.4 **Proportionality**

If the activities are necessary, the person granting the authorisation must believe that they are proportionate to what is sought to be achieved by carrying them out. This involves balancing the intrusiveness of the activity on the target and others who might be

affected by it against the need for the activity in operational terms. The activity will not be proportionate if it is excessive in the circumstances of the case or if the information which is sought could reasonably be obtained by other less intrusive means. All such activity should be carefully managed to meet the objective in question and must not be arbitrary or unfair. A useful summary on proportionality is:

1. Is use of Covert Surveillance **proportionate to the crime** being investigated?

2. Is the surveillance aim **proportionate to the degree of anticipated intrusion** on the target or others?

3. Is it the only option? **Have Overt means been considered** and discounted?

8.5 **Authorisation**

All Directed Surveillance shall be authorised, **in writing**, in accordance with this procedure. If an authorisation is refused, this should still be sent through to legal as the Central Record should contain refusals as well as authorised surveillance.

8.6 **Urgent Authorisations for Directed Surveillance**

Due to the Magistrates approval process a Local Authority can no longer seek urgent oral authorisations. In circumstances where the Applicant considers there is some urgency, they should first consider whether the immediate response provisions of **section 26(2)(c) of *RIPA*** apply. Alternatively it may be appropriate to contact the Police as they still retain this power.

8.7 **Duration for Directed Surveillance**

Authorisation for Directed Surveillance must be reviewed in the time stated and cancelled immediately it is no longer required.
Directed Surveillance Authorisations to carry out/conduct Surveillance are valid for 3 months duration from the date of Authorisation unless cancelled or renewed. The Authorisation forms must be cancelled and/or renewed during the 3 month period. The validity of the forms and their related authorisations is not dependent upon whether actual surveillance is carried out/conducted or not, as the forms do not cease to be valid after 3 months because they must either be cancelled or renewed within this period.

8.8 Authorisations can be renewed in writing when the maximum period has expired. The Authorising Officer must consider the matter afresh, including taking into account the benefits of the surveillance to date, and any collateral intrusion that has occurred. The renewal must also be authorised by the Magistrates before being acted upon.

8.9 The renewal will begin on the day when the authorisation would have expired.

9. Time Periods for Authorisations for Directed Surveillance

Written authorisations for directed surveillance expire 3 months beginning on the day from which they took effect; that being the day of the Magistrates approval.

10. Time Periods for Renewals for Directed Surveillance

10.1 If at any time before an authorisation would expire the Authorising Officer considers it necessary for the authorisation to continue for the purpose for which it was given, it may be renewed in writing for a further period of 3 months beginning with the day on which the original or previous authorisation ceases to have effect. Applications for renewals should only be made shortly before the authorisation is due to expire. The renewals must be authorised by a Magistrate.

10.2 Any person entitled to authorise applications may renew authorisations. Applications may be renewed more than once, provided they continue to meet the criteria for authorisation.

11. Review of Ongoing Authorisations for Directed Surveillance

11.1 The Authorising Officer must review all authorisations at intervals of not more than 4 weeks. Details of the review and the decision reached shall be documented on the original application and recorded using the review form.

12. Cancellation of Directed Surveillance Authorisation

12.1 The Authorising Officer must cancel an authorisation if he/she is satisfied that the Directed Surveillance no longer satisfies the criteria for authorisation, or at the point where all information sought has been obtained.

12.2 There is nothing in the ***RIPA*** which prevents material obtained from properly authorised surveillance from being used in other investigations. Each Public Authority must ensure that arrangements are in place for the handling, storage and destruction of material obtained through the use of Covert Surveillance. Authorising Officers must 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.

13. Obtaining a Unique Reference Number for Directed Surveillance

Each Application form must be identified with a **Unique Reference Number (URN)** which is allocated by Legal Services. The Authorising Officer /Applicant should phone/email Legal Services as soon as possible to obtain the next available URN. Any Surveillance refused by the Authorising Officer should also have a URN and be provided to Legal Services. If an amended request for authorisation is made for the same matter, the same URN can be used so that the matter can be tracked.

PROCEDURE RELATING TO THE DEPLOYMENT OF A COVERT HUMAN INTELLIGENCE SOURCE (*CHIS)*

14. Due to the unique and onerous responsibilities relating to the deployment of a ***CHIS,*** an Applicant must first seek Legal Advice from Legal Services (**Senior Responsible Officer** or ***RIPA*** **Coordinating Officer**) before applying for the authorisation of a ***CHIS***.

14.1 ***CHIS*** **- definition**

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

14.2 Using a ***CHIS*** should not be undertaken lightly as the Authority will have an ongoing duty of care to that person due to the situation they have been placed in. It is therefore essential that a risk assessment takes place before a ***CHIS*** is deployed.

14.3 ***RIPA*** does not apply in circumstances where members of the public volunteer information to the **DMBC** as part of their normal civic duties, or to contact numbers set up to receive information. However both these situations need to be managed carefully as the Authority asking for further information or encouraging the informant to report back again is likely to lead to the informant becoming a surveillance agent or a ***CHIS***.

14.4 **SPECIFIC REQUIREMENTS FOR *CHIS* AUTHORISATION**

The Conduct or Use of a ***CHIS*** requires prior authorisation.

- **Conduct** of a ***CHIS*** means: 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*** means: Any action, **inducing, asking or assisting** a person to act as a ***CHIS*** and the decision to use a CHIS in the first place.

14.5 **PLEASE NOTE DMBC** is only **Permitted by Law** to use a ***CHIS*** if ***RIPA*** procedures are **RIGOROUSLY FOLLOWED** as set out in this document.

ADVICE MUST ALWAYS BE OBTAINED FROM LEGAL SERVICES BEFORE A *CHIS* IS DEPLOYED

14.6 **Juvenile Sources**

Special safeguards apply to the use or conduct of Juvenile Sources (i.e. under 18 years). 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 or Deputy are duly authorised by the **DMBC** to use Juvenile Sources, as other more onerous requirements will need to be complied with.

14.7 **Vulnerable Individuals**

A Vulnerable Individual is a person who is or may be in need of community care services by reason of mental or other disability, age or illness and who is or may be unable to take care of himself or herself, or unable to protect himself or herself against significant harm or exploitation. A Vulnerable Individual will only be authorised to act as a covert human intelligence source in the most exceptional of circumstances. Only the Chief Executive or Deputy, are allowed by the DMBC to authorise the use of Vulnerable Individuals as a ***CHIS***, due to the need to comply with additional more onerous requirements.

14.9 **Test Purchases**

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 test 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).

14.10 By contrast, developing a relationship with a person in the shop, to obtain information about the seller's suppliers of an illegal item. (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** **Directed Surveillance**.

14.11 **Anti-Social Behaviour Activities (e.g. noise)**

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.

14.12 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 noise maker has been warned that this will occur. Placing a stationary or mobile video camera outside a building to record anti social behaviour on residential estates will require prior authorisation.

15. *CHIS* AUTHORISATION PROCEDURE

15.1 The use of ***CHIS*** can only be lawfully carried out if properly authorised and in strict accordance with the terms of the authorisation.

15.2 **Authorised Officers and Magistrates Approval**

Forms can only be signed by trained Authorising Officers. A Central List of Authorised Officers will be retained by the Head of Legal Services. This list will be kept up-to-date using the notification procedure. All Authorising Officers should have adequate training relating to compliance with ***RIPA*** implementation and be fully conversant with the content of this procedural document.

15.3 Authorising Officers within the meaning of this procedure should avoid authorising their own activities. A ***CHIS*** is **NOT PERMITTED** to authorise their own activities.

15.4 **Authorisations must be in writing**. Once the form has been signed Legal Services should be consulted to ensure the correct process has been complied with. Upon receipt of Legal Services approval the Applicant should personally contact the Magistrates Court to arrange an appointment with a Magistrate to approve the surveillance application documents.

15.5 ***CHIS*** **Application Forms**

All applications for ***CHIS*** authorisations will be made on official designated stationery, which accords with the Code of Practice. The applicant in all cases should always complete this in person.

15.6 **Duration**

The Authorisation must be renewed in the time stated and cancelled once it is no longer needed. The Authorisation to conduct the Surveillance lasts for 12 months for ***CHIS*** unless cancelled or renewed.

15.7 At the end of 12 months, if the need for the information continues and this is deemed to be the only way that it can be obtained, the original Authorisation can be renewed and this will need to be placed before a Magistrate before it is effective. This is a prescribed process under the ***RIPA*** **Code of Practice** which **MUST** be followed.

15.8 Where Authorisation ceases to be either necessary or appropriate, the Authorising Officer **MUST** cancel an authorisation.

15.9 All Authorisations must be reviewed **(at least every 4 weeks)** from the date of authorisation, and must be attached to the **original authorisation.**

15.10 The respective **Forms, Code of Practice and Supplementary Material** is available on the Council Intranet, or directly from Legal Services.

15.11 Services wishing to adopt a more devolved authorisation process may do so only on the explicit approval of a written policy by the Council; all authorisations must remain within the scope of the Code of Practice relating to persons permitted to give authorisation.

15.12 All applications for ***CHIS*** should accord with the ***CHIS*** **Code of Practice.** The necessary forms are the **Application, Review, Renewal** and **Cancellation**

16. Authorisation Criteria

16.1 Prior to granting an Authorisation for ***CHIS***, the Authorising Officer must be satisfied that:-

- the authorisation is for a **prescribed lawful purpose** (i.e. the prevention or detection of crime or the prevention of disorder);
- the purpose of the use of a ***CHIS*** is **clearly defined and stated**.
- account has been taken of the likely **degree of intrusion** into the privacy of persons other than those directly implicated in the operation or investigation (called **'Collateral Intrusion'**). Measures must be taken, wherever practicable, to avoid unnecessary intrusion into the lives of those affected by Collateral Intrusion. These measures and extent of possible intrusion should be recorded on the form;
- the authorisation is **necessary**;
- the authorised surveillance action is **proportionate** to the information being sought;
- any **equipment** to be used is **specified**;
- the information required cannot be obtained by **alternative methods.**
- A **risk assessment** has been completed.

16.2 **Necessity for *CHIS***

Surveillance operations shall only be undertaken where there is no reasonable and effective alternative way of achieving the desired objective(s).

16.3 **Effectiveness of *CHIS***

Surveillance Operations shall be undertaken only by suitably trained or experienced employees, or under their direct supervision.

16.4 **Proportionality for *CHIS***

The use of surveillance shall not be excessive, i.e. it shall be in proportion to the significance of the matter being investigated. A useful test is:

1. Is use of Covert Surveillance proportionate to the mischief being investigated?

2. Is the surveillance aim proportionate to the degree of anticipated intrusion on the target or others?

3. Is it the only option? Have Overt means been considered and discounted?

16.5 **Authorisation for *CHIS***

All ***CHIS*** shall be authorised, **in writing**, in accordance with this procedure.
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 **necessary and 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; and

(f) ensure that there is an **appointment of a Controller, Handler and Record Keeper** in each case. The person referred to in **section 29(5)(a)** of the **2000 Act (** the **"Handler")** will have day to day responsibility for:

- dealing with the ***CHIS*** on behalf of **The Authority** concerned;
- directing the day to day activities of the ***CHIS***;
- recording the information supplied by the ***CHIS***; and
- monitoring the security and welfare of the ***CHIS***.
- The Handler of a ***CHIS*** will usually be of a rank or position below that of the Authorising Officer. The person referred to in **section 29(5)(b)** of the **2000 Act (**the **"Controller")** will normally be responsible for the management and supervision of the "**Handler**" and general oversight of the use of the ***CHIS***.

16.6 **Urgent Authorisations for use of a *CHIS***

Due to the changes in the Law requiring the approval of a Magistrate, Local Authorities are **no longer permitted** to seek **Urgent Oral Authorisation**. In circumstances which the Applicant considers there is some urgency they should first consider whether the immediate response provisions of ***RIPA*** apply under **section 26(2)(c) of the *RIPA* Regulations** (unlikely with a ***CHIS***). Alternatively it may be appropriate to contact the Police as they still retain this power.

16.7 ***CHIS* Duration**

The Authorisation must be reviewed in the time stated and cancelled once it is no longer needed. The 'Authorisation' to carry out/conduct the surveillance for a ***CHIS*** lasts for a maximum of 12 months (from authorisation). However, whether the surveillance is actually carried out/conducted or not, during the relevant period, does not mean the 'authorisation' becomes 'spent'. In other words, the Forms and their related authorisations) do not expire. The forms have to be reviewed and/or cancelled (once they are no longer required).

16.8 Authorisations can be renewed in writing when the maximum period has expired. The Authorising Officer must consider the matter afresh, including taking into account the benefits of the surveillance to date, and any Collateral Intrusion that has occurred. The Renewals will only be effective once authorised by a Magistrate.

16.9 The renewal will begin on the day when the authorisation would have expired.

17. *CHIS* Time Periods for Authorisations

17.1 Written authorisations for CHIS expire 12 months beginning on the day from which they took effect.

18. *CHIS* Time Periods for Renewals

18.1 If at any time before an authorisation would expire the authorising officer considers it necessary for the authorisation to continue for the purpose for which it was given, it may be renewed in writing for a further period of 12 months beginning with the day on which the original or previous authorisation ceases to have effect. Applications for renewals should only be made shortly before the authorisation is due to expire. Approval of a Magistrate is necessary before it will be effective.

18.2 Any person entitled to authorise applications may apply to renew authorisations. Applications may be renewed more than once, provided they continue to meet the criteria for authorisation. All renewals require approval of a Magistrate.

19. Review of Ongoing Authorisations of *CHIS*

The Authorising Officer must review all authorisations at intervals of **not more than 4 weeks.** Details of the review and the decision reached shall be documented on the original application and recorded using the review form.

20. Cancellation of Authorisation of CHIS

The Authorising Officer must cancel an authorisation if he/she is satisfied that the Directed Surveillance no longer satisfies the criteria for authorisation, or at the point where all information sought has been obtained.

21. *CHIS* Unique Reference Number (URN).

Each form must have a Unique Reference Number allocated by Legal Services. The Authorising Officer/Applicant should phone/email Legal Services as soon as possible to be allocated the next available URN.

22. Investigations involving Social Media

22.1 Social Media sites are a useful tool for intelligence and evidence gathering. However there is a fine distinction between accessing readily available personal information posted into the public domain on Social Media and interfering in an individual's private life. The Internet is a surveillance device as defined by **section 48(1) *RIPA*.**

Surveillance is **Covert** "**<u>if, and only if</u>**, it is conducted in a manner that is calculated to ensure that persons who are subject to the surveillance are unaware that it is, or may be taking place." Knowing that something is capable of happening is not the same as an awareness that it is or may be taking place.

22.2 Reviewing open source sites does not require authorisation unless the review is carried out with some regularity, usually when creating a profile, in which case directed surveillance authorisation will be required. If it becomes necessary to breach the privacy controls and become for example 'a friend' on the Facebook site, with the investigating officer utilising a false account concealing his/her identity as a council officer for the purposes of gleaning intelligence , this is a covert operation intended to obtain private information and should be authorised , at the minimum , as directed surveillance. If the investigator engages in any form of relationship with the account operator then they become a CHIS requiring authorisation as such and management by a Controller and Handler with a record being kept and a risk assessment created.

22.3 The use of Social Media for the gathering of evidence to assist in enforcement activities should be used with the following considerations:

- It is only in the most exceptional cases that a false identity should be used in order to 'friend' individuals on social networks and ***RIPA*** Authorisation must always be obtained. A possible use may be to investigate the sale of counterfeit goods on Social Media site where there is no other method of obtaining evidence.

- Officers viewing an individual's open profile on a social network should do so only in order to obtain evidence to support or refute their investigation; this should only be done to obtain the information and if necessary later to confirm the information.

- Systematic viewing of a profile will normally amount to surveillance and a ***RIPA*** Authorisation should be obtained.

- ***RIPA*** should also be considered where a friend request is sent or if a conversation has been entered into the with the owner of the page as this may amount to a ***CHIS.***

- Officers should be aware that it may not be possible to verify the accuracy of information on social networks and, if such information is to be used as evidence, reasonable steps must be taken to ensure its validity.

23. Monitoring

23.1 Each Service must maintain a record of all applications for authorisation (including refusals), renewals, reviews and cancellations. This **record must be used** to ensure authorisations are subsequently reviewed, renewed or cancelled.

23.2 At least annually the Council's arrangements will be reviewed and a report submitted to the Audit Committee. **Interim Update** reports shall be delivered to the Committee at intervals of approximately six months.

24. Training and Training Records

24.1 Directors shall arrange for all officers regularly involved in the use of ***RIPA*** to receive appropriate training. Authorising Officers must receive regular training on ***RIPA*** and **Council Procedures**.

24.2 The Directors shall ensure that appropriate records of such training is retained so that it may be produced at a ***RIPA*** **Surveillance Commissioner Inspection.**

25. Working in conjunction with Other Agencies

25.1 When some other agency has been instructed to undertake any action under ***RIPA*** on behalf of the DMBC, this Document and the Council Forms **MUST** be used (as per normal procedure). The agency should be advised or kept informed of any specific requirements as necessary. Any agent must be made explicitly aware of the scope and limitation of their authority to protect DMBC against any breach of the ***RIPA*** related provisions.

25.2 When any external agency (e.g. Police, Customs & Excise, Inland Revenue, etc.):-

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

(b) wish to use any premises controlled by **DMBC** 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 why the those premises should not be used for the agency's activities. Suitable insurance or other appropriate indemnities may be sought from the other agency to secure co-

operation from **DMBC** in the agent's **RIPA** operation. The ***RIPA*** Forms and documentation normally used by the **DMBC** should not be used in such cases, however, as the **DMBC** is only 'assisting' and not being 'involved' in the **RIPA** activity of the external agency.

25.3 In terms of 24.2(a) above, if the Police or other Agency wish to use **DMBC** resources for General Surveillance, as opposed to Specific ***RIPA*** Operations, a letter detailing the proposed use, extent of remit, duration, and identity of the person responsible for undertaking the general surveillance and the purpose of the operation must be obtained from the Police or other Agency before any **DMBC** resources are made available for the proposed use.

25.4 **IF THERE IS ANY REASON FOR DOUBT OR UNCERTAINTY REGARDING PROCEDURAL ISSUES**, please consult with the Head of Legal Services at the earliest opportunity.

26. Security and Retention of Documents

Documents created under this procedure are **Highly Confidential** and shall be treated as such. Services shall make proper arrangements for their retention, security and destruction, in accordance with the requirements of the **Data Protection Act 1998 and the Codes of Practice.**

27. Internal Overview, Equipment and Records Management

27.1 **Senior Responsible Officer (SRO)** is the **Assistant Director – Legal and Democratic Services**. The **SRO** has the Legal Responsibility on behalf the Authority for **RIPA** related activity and fulfils a recommendation in the **Directed Surveillance** and ***CHIS*** **Code of Practice**, including responsibility to ensure that all Authorising Officers are trained to the appropriate standard and is liable to remedy any concerns highlighted by any **Inspection Report from the Office of the Surveillance Commissioners**. The Assistant Director regularly attends Corporate Leadership Team meetings in accordance with the requirements of the ***RIPA*** **Codes of Practice.**

27.2 **RIPA Coordinating Officer.**

A Principal Legal Officer **(PLO)** for the Authority undertakes the role of the ***RIPA*** **Coordinating Officer** whose duties include:

a) Ensuring maintenance of the the Central Record of Authorisations and collating the original applications/authorisation, reviews, renewals and cancellations.

b) Oversight of submitted ***RIPA*** documentation.

c) Organising a ***RIPA*** training programme.

d) Raising ***RIPA*** awareness with in the Council.

e) Ensuring a **URN** is correctly allocated.

Due to the Oversight Role of the Coordinating Officer he/she cannot also be an Authorising Officer.

27.3 **Councillor Overview Role**

The Codes also require that:

a) Councillors should review the use of ***RIPA*** by **DMBC** and also review the policy at least once a year;

b) Councillors should also consider internal reports on use of ***RIPA*** on a regular basis to ensure that it is being used consistently in accordance with the Council's Policy and to ensure that the policy remains fit for purpose. They should not be involved in making decisions on specific authorisations.

27.4 **Head of Paid Service**

The Code also requires that the authorisation level when knowledge of Confidential Information is likely to be acquired or when a vulnerable individual or juvenile is to be used as a ***CHIS*** source must be the Head of Paid Service or (in their absence) the person acting as the Head of Paid Service. Doncaster Council's Constitution specifically states that the Assistant Director – Legal and Democratic Services is to act in this role in the absence of the Head of Paid Service.

27.5 **Records**

The DMBC must keep a detailed record of all authorisations, renewals, cancellations and rejections in Departments and a Central Register of all Authorisation Forms will be maintained and monitored by the Senior Responsible Officer **(SRO).**

27.6 **Central Register maintained by the Head of Legal Services**

Authorised Officers MUST forward each original authorisation form along with the pro forma (Appendix 3) and then each renewal or cancellation form to the Head of Legal Services for the Central Register, **WITHIN 1 week of the authorisation, review, renewal, cancellation or rejection.** Authorised Officers must ensure when

sending the originals of any forms to the Head of Legal Services they are sent in sealed envelopes and marked '**Strictly Private and Confidential**'. The Head of Legal Services will monitor the same and give appropriate guidance, from time to time, or amend this Document, as necessary.

27.7 **DMBC** will retain records for a period of at least three years from the ending of the authorisation or until the next OSC Inspection if longer. The Office of the Surveillance Commissioners (OSC) can audit/review **DMBC's** policies and procedures, and individual authorisations.

27.8 **Records maintained in the Department**

The following documents must be retained by the relevant Heads of Service (or his/her Designated Officer) for such purposes.

- copy 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 documentations submitted when the renewal was requested;
- the Date and Time when any instruction was given by the Authorising officer;
- the Unique Reference Number for the authorisation (URN).

Documents should be retained for a minimum of three years from the ending of the authorisation. Documentation should be securely maintained, with limited access, to ensure confidentiality is not breached.

27.9 Each form will have a URN. These are allocated by Legal Services (see 14).

27.10 **Equipment Register**

An Equipment Register is maintained by the RIPA Coordinating officer of all equipment that the Council holds for the purposes of Covert Surveillance. This lists the names of the Responsible Officers for each piece of equipment who will ensure that an equipment log is kept detailing equipment in/out and the URN that the equipment is being

used for. Any changes to the equipment kept should be notified by the responsible persons listed to the RIPA Coordinating Officer. The log in/out of equipment should be retained and available for any check by the ***RIPA*** Coordinating Officer, Senior Responsible Officer and Surveillance Commissioners.

28. External Overview

28.1 The Office of Surveillance Commissioners provides an independent overview of the use of the powers contained within the Regulation of Investigatory Powers Act 2000. This scrutiny includes inspection visits to local authorities by Inspectors appointed by the Office of the Surveillance Commissioners.

28.2 It is anticipated that the inspectors will speak to the Head of Legal Services and the Central Corporate co-ordinator.

28.3 Inspections can take place unannounced.

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

28.5 The European Convention did not, however, make this an absolute right, but a qualified right. Accordingly, in certain circumstances, the DMBC may interfere in the citizen's right 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).

28.6 The Regulation of Investigatory Powers Act 2000 ('***RIPA***') provides a statutory mechanism (i.e. 'in accordance with the law') for authorising covert surveillance and the use of a 'Covert Human Intelligence Source' ('***CHIS***') - e.g. undercover agents. It 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.

28.7 Directly employed Council staff and external agencies working for the DMBC are covered by the Act for the time they are working for the DMBC. 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 Authorised Officers.

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

29. Use of covert surveillance outside of RIPA

29.1 ***RIPA*** legislation is permissive i.e. it gives a Local Authority reassurance that in carrying out Covert Surveillance that it is not breaching **The Human Rights Act 1998**. In very unique and specific circumstances it may be possible to lawfully carry out surveillance outside of the ***RIPA*** legislation. This will require a procedure to be followed very similar to that used for ***RIPA*** authorisations. The **SRO** and the Coordinating Officer must be consulted before any such surveillance is considered.

30. Complaints

30.1 The **Regulation of Investigatory Powers Act 2000** establishes an Independent Tribunal. This has full powers to investigate and decide any cases within its jurisdiction.

30.2 The Council will ensure that copies of the Tribunal's information sheet, their complaint form and their Human Rights Act claim form will be made available on request at all main Council public offices.

30.3 Copies of the **RIPA Code of Practice** and **Council Policy Statement** will be supplied on request from anyone seeking a copy.

Drafted - April 2003

1st Amendment - April 2004

2nd Amendment - March 2008

3rd Amendment - September 2009

4th Amendment - November 2012

5th Amendment - May 2013

6th Amendment - December 2014

7th Amendment - March 2016