Appendix 1
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)

Contents

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 required; where appropriate council internal forms should be used for access to email and internet information and where necessary the non-RIPA procedure (see 28.1) may be used following consultation with the RIPA Coordinating Officer in Legal Services.

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 managers in the following departments:

- Legal
- Trading Standards
- Enforcement

2. Objective of This Procedure

2.1 The objective of this procedure is to ensure that all work involving Directed Surveillance and Covert Human Intelligence Sources 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 Home Office Codes of Practice relating to the Use of Covert Human Intelligence Sources and Directed Surveillance, which are 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 POTENTIALLY SERIOUS LEGAL CONSEQUENCES ARE AVOIDED.

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; and

- 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 making general observations).

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*).

Whilst a person may have a reduced expectation of privacy when in a public place, covert surveillance of that person's activities in public may still result in the obtaining of private information. This is likely to be the case where that person has a reasonable expectation of privacy even though acting in public and where a record is being made by a public authority of that person's activities for future consideration or analysis. Surveillance of publicly accessible areas of the internet should be treated in a similar way, recognising that there may be an expectation of privacy over information which is on the internet, particularly where accessing information on social media websites.

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;
- 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 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 officer carrying out such 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. If there is a need to access employee computer and phone records advice should be sought from human resources and / or internal audit. The Information Commissioner's Office 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. They must be at least the rank of Service Manager or above and have been suitably trained. The current list of Authorising Officers is available on the Legal & Democratic Services intranet page.

3.7 **Private information** includes information about a person relating to his private or family life (see paragraph 3.4 above).

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.

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.

3.11 **Senior Responsible Officer** is the Assistant Director of Legal & Democratic Services.

3.12 **RIPA Co-ordinating Officer** is the Principal Legal Officer (Education and Litigation Team) in Legal & Democratic Services.

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 fly tipping controlled waste. - A test purchase where the purchaser is wearing recording equipment, or an Council Officer is observing
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 Senior Responsible Officer or RIPA Co-ordinating Officer 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) Order 2010.

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);
- confidential journalistic material; or
- material relating to the constituency business of Members of Parliament.

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 Assistant Director of Legal & Democratic 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 raised with Legal Services.

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 Legal & Democratic Services page on the intranet and MUST be personally completed by the applicant in all circumstances.

7.6 **Period of Validity of Authorisations**

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 immediately cancel an authorisation, using the cancellation form.

7.10 All authorisations must be reviewed at least every 4 weeks from the date of authorisation, using the review form, which must be attached to the original authorisation.

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

8. Authorisation Criteria for Directed Surveillance

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. In order to give proper consideration to collateral intrusion, an authorising officer or person considering issuing the authorisation should be given full information regarding the potential scope of the anticipated surveillance, including the likelihood that any equipment or software deployed may cause intrusion on persons or property other than the subject(s) of the application. If an automated system such as an online search engine is used to obtain the information, the authorising officer should be made aware of its potential extent and limitations. Material which is not necessary or proportionate to the aims of the operation or investigation should be discarded or securely retained separately where it may be required for future evidential purposes. The authorising officer or person considering issuing the authorisation should ensure appropriate safeguards for the handling, retention or destruction of such material in accordance with the codes of practice and data protection requirements. Please refer to the Council's Data Protection Policy, Law Enforcement (Data Protection) Policy, and Information Security Policy. 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; and

- 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 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 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. The case for an authorisation should be presented in the application in a fair and balanced way. In particular, all reasonable efforts should be made to take account of information which supports or weakens the case for the authorisation. If an authorisation is refused, this should still be sent through to Legal Services 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. <u>Time Periods for Directed Surveillance</u>

9.1 **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. Even in instances where it is anticipated that an authorisation will only be required for a period of time less than three months, authorisation should still be granted for the statutory three month period, subject to review at an interval reflecting expected duration (and in any event at least every four weeks), and the authorisation cancelled immediately when it is no longer necessary.

9.2 **Time Periods for Renewals for Directed Surveillance**

9.2.1 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.

9.2.2 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.

9.3 **Review of Ongoing Authorisations for Directed Surveillance**

9.3.1 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. During a review, the reviewing officer may amend aspects of the authorisation for example to cease directed surveillance against one of a number of named subjects or to discontinue the use of a particular tactic.

10. Cancellation of Directed Surveillance Authorisation

10.1 The Authorising Officer must immediately 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.

10.2 There is nothing in the ***RIPA*** which prevents material obtained from properly authorised surveillance from being used in other investigations. However, the material must be processed in accordance with the safeguards set out in paragraph 19 below. Authorising Officers must also ensure compliance with the appropriate data protection requirements.

11. 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.

12. Procedure Relating To The Deployment Of A Covert Human Intelligence Source (*CHIS)*

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*.

12.1 ***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.

12.2 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.

12.3 *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*.

12.4 **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.

12.5 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

12.6 **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.

12.7 **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.

12.8 **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).

12.9 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.

12.10 **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.

12.11 Recording sound (with A DAT recorder) on private premises could constitute Intrusive Surveillance, unless it is done overtly. For example, it will be possible to record sound if the 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.

13. *CHIS* Authorisation Procedure

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

13.2 **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.

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

13.4 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.

13.5 ***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.

13.6 **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.

13.7 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.

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

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

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

13.11 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.

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

14. Authorisation Criteria

14.1 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.

14.2 **Necessity for *CHIS***

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

14.3 **Effectiveness of *CHIS***

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

14.4 **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?

14.5 **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*.

14.6 **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.

14.7 ***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).

14.8 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.

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

15. *CHIS* Time Periods

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

15.2. ***CHIS* Time Periods for Renewals**

15.2.1 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.

15.2.2 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.

15.3 **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.

15.4 **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.

16. *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.

17. Online Covert Activity and Investigations involving Social Media

17.1 The internet provides a useful tool for intelligence and evidence gathering. It is important that public authorities are able to make full and lawful use of this information for their statutory purposes. Much of it can be accessed without the need for RIPA authorisation; use of the internet prior to an investigation should not normally engage privacy considerations. But if the study of an individual's online presence becomes persistent, RIPA authorisations may need to be considered. 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 "if, and only if, 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.

17.2 Whether a public authority interferes with a person's private life includes a consideration of the nature of the public authority's activity in relation to that information. Simple reconnaissance of such sites (i.e. preliminary examination with a view to establishing whether the site or its contents are of interest) is unlikely to interfere with a person's reasonably held expectation of privacy and therefore is not likely to require a directed surveillance authorisation. But where a public authority is systematically collecting and recording information about a particular person or group, a directed surveillance authorisation should be considered. These considerations apply regardless of when the

information was shared online. 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.

17.3 Depending on the nature of the online platform, there may be a reduced expectation of privacy where information relating to a person or group of people is made openly available within the public domain, however in some circumstances privacy implications still apply. This is because the intention when making such information available was not for it to be used for a covert purpose such as investigative activity. This is regardless of whether a user of a website or social media platform has sought to protect such information by restricting its access by activating privacy settings. In deciding whether online surveillance should be regarded as covert, consideration should be given to the likelihood of the subject(s) knowing that the surveillance is or may be taking place. Use of the internet itself may be considered as adopting a surveillance technique calculated to ensure that the subject is unaware of it, even if no further steps are taken to conceal the activity. Conversely, if reasonable steps have been taken to inform the public or particular individuals that the surveillance is or may be taking place, this can be regarded as overt and a directed surveillance authorisation will not normally be available.

17.4 In order to determine whether a directed surveillance authorisation should be sought for accessing information on a website as part of a covert investigation or operation, it is necessary to look at the intended purpose and scope of the online activity it is proposed to undertake. Factors that should be considered in establishing whether a directed surveillance authorisation is required include:

- Whether the investigation or research is directed towards an individual or organisation.

- Whether it is likely to result in obtaining private information about a person or group of people.

- Whether it is likely to involve visiting internet sites to build up an intelligence picture or profile.

- Whether the information obtained will be recorded and retained.

- Whether the information is likely to provide an observer with a pattern of lifestyle.

- Whether the information is being combined with other sources of information or intelligence, which amounts to information relating to a person's private life.

- Whether the investigation or research is part of an ongoing piece of work involving repeated viewing of the subject(s).

- Whether it is likely to involve identifying and recording information about third parties, such as friends and family members of the subject of interest, or information posted by third parties, that may include private information and therefore constitute collateral intrusion into the privacy of these third parties.

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

- 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.

17.5 Where a Council Officer or member of the public is tasked by the Council to use an internet profile to establish or maintain a relationship with a subject of interest for a covert purpose, or otherwise undertakes such activity on behalf of the public authority, in order to obtain or provide access to information, a CHIS authorisation is likely to be required. For example:

- An investigator using the internet to engage with a subject of interest at the start of an operation, in order to ascertain information or facilitate a meeting in person.

- Directing a member of the public (such as a CHIS) to use their own or another internet profile to establish or maintain a relationship with a subject of interest for a covert purpose.

- Joining chat rooms with a view to interacting with a criminal group in order to obtain information about their criminal activities

A CHIS authorisation will not always be appropriate or necessary for online investigation or research. Some websites require a user to register providing personal identifiers (such as name and phone number) before access to the site will be permitted. Where a Council officer sets up a false identity for this purpose, this does not in itself

amount to establishing a relationship, and a CHIS authorisation would not immediately be required, though consideration should be given to the need for a directed surveillance authorisation if the conduct is likely to result in the acquisition of private information, and the other relevant criteria are met.

Where a website or social media account requires a minimal level of interaction, such as sending or receiving a friend request before access is permitted, this may not in itself amount to establishing a relationship. Equally, the use of electronic gestures such as “like” or “follow” to react to information posted by others online would not in itself constitute forming a relationship. However, it should be born in mind that entering a website or responding on these terms may lead to further interaction with other users and a CHIS authorisation should be obtained if it is intended for an officer or a CHIS to engage in such interaction to obtain, provide access to or disclose information.

Where covert surveillance is being considered by using the internet the Home Office Codes of Practice sections entitled ‘Online Covert Activity’ should be read in full. Internet searches carried out by a third party on behalf of a public authority, or with the use of a search tool, may still require a directed surveillance authorisation

18. Aerial Covert Surveillance

Where surveillance using airborne crafts or devices, for example helicopters or unmanned aircraft (colloquially known as ‘drones’), is planned, the considerations set out in paragraphs 3 and 5 of the Home Office Covert Surveillance Code of Practice should be considered as to whether a directed surveillance authorisation is appropriate. In considering whether the surveillance should be regarded as covert, account should be taken of the reduced visibility of a craft or device at altitude.

19. Safeguards in regard to material/information acquired.

The Home Office Covert Surveillance Code of Practice provides detailed guidance at Section 9 which should be read. In summary:

19.1 Lawful, justified and strictly controlled

Public authorities should ensure that their actions when handling Information obtained by means of covert surveillance or property interference comply with relevant legal frameworks and this code so that any interference with privacy is justified in accordance with Article 8(2) of the European Convention on Human Rights. Compliance with these legal frameworks, including data protection requirements, will ensure that the handling of private information so obtained continues

to be lawful, justified and strictly controlled, and is subject to robust and effective safeguards.

19.2 **Safeguards**

All material obtained under the authority of a covert surveillance authorisation must be handled in accordance with safeguards which the Council has in place in its policies, in particular in the Data Protection Policy, the Law Enforcement (Data Protection) Policy and the Information Security Policy. These safeguards will be made available to the Investigatory Powers Commissioner (IPC) if requested. Doncaster Council will keep its internal safeguards as set out in those policies under periodic review to ensure that they remain up-to-date and effective.

19.3 **Use of material kept to the minimum necessary**

Dissemination, copying and retention of material must be limited to the minimum necessary for authorised purposes. Something is necessary for the authorised purposes if the material:

- is, or is likely to become, necessary for any of the statutory purposes set out in RIPA in relation to covert surveillance;
- is necessary for facilitating the carrying out of the functions of the Council under RIPA;
- is necessary for facilitating the carrying out of any functions of the Commissioner or the Investigatory Powers Tribunal;
- is necessary for the purposes of legal proceedings; or
- is necessary for the performance of the functions of any person by or under any enactment.

19.4 **Use of material as evidence**

Material obtained through directed surveillance may be used as evidence in criminal proceedings. Ensuring the continuity and integrity of evidence is critical to every prosecution. Accordingly, considerations as to evidential integrity are an important part of the disclosure regime under the Criminal Procedure and Investigations Act 1996 and these considerations will apply to any material acquired through covert surveillance that is used in evidence. When information obtained under a covert surveillance authorisation is used evidentially, Doncaster Council should be able to demonstrate how the evidence has been obtained, to the extent required by the relevant rules of evidence and disclosure. Where the product of surveillance could be relevant to

pending or future criminal or civil proceedings, it should be retained in accordance with Doncaster Council's established disclosure requirements.

19.5 **Handling Material**

Authorising officers, must ensure compliance with the appropriate data protection requirements under the Data Protection Act 2018 and the General Data Protection Regulation and Doncaster Council's Data Protection, Law Enforcement (Data Protection) and Information Security Policies.

19.6 **Dissemination of Information**

Material acquired through covert surveillance will need to be disseminated both within Doncaster Council and with other public authorities, where necessary in order for action to be taken on it. The number of persons to whom any of the information is disclosed, and the extent of disclosure, should be limited to the minimum necessary for the authorised purpose(s). This obligation applies equally to disclosure to officers within Doncaster Council and to disclosure outside the authority. In the same way, only so much of the material may be disclosed as the recipient needs; for example if a summary of the material will suffice, no more than that should be disclosed.

19.7 **Copying**

Material obtained through covert surveillance may only be copied to the extent necessary for the authorised purpose. Copies include not only direct copies of the whole of the material, but also extracts and summaries which identify themselves as the product of covert surveillance, and any record which refers to the covert surveillance and the identities of the persons to whom the material relates.

19.8 **Storage**

Material obtained through covert surveillance, and all copies, extracts and summaries of it, must be handled and stored securely, so as to minimise the risk of loss or theft. It must be held so as to be inaccessible to persons without the required level of security clearance (where applicable). This requirement to store such material securely applies to all those who are responsible for the handling of the material.

19.9 **Destruction**

Information obtained through covert surveillance and all copies, extracts and summaries thereof, should be scheduled for deletion or destruction and securely destroyed in accordance with Doncaster Council's retention policy.

20. Confidential or privileged material

Particular consideration should be given in cases where the subject of the investigation might reasonably assume a high degree of confidentiality. This includes where the material contains information that is legally privileged, confidential journalistic material or where material identifies a journalist's source, where material contains confidential personal information or communications between a Member of Parliament and another person on constituency business. Directed surveillance likely or intended to result in the acquisition of knowledge of confidential or privileged material may be authorised only by authorising officers entitled to grant authorisations in respect of confidential or privileged information which for Doncaster Council is the Chief Executive (or their appointed deputy).

20.1 Confidential personal information and communications of a Member of Parliament

Confidential personal information is information held in confidence concerning an individual (whether living or dead) who can be identified from it, and the material in question relates to his physical or mental health or to spiritual counselling. Such information can include both oral and written communications. Such information as described above is held in confidence if it is held subject to an express or implied undertaking to hold it in confidence or it is subject to a restriction on disclosure or any legal obligation of confidentiality. Confidential constituent information is information relating to communications between a Member of Parliament and a constituent in respect of constituency business. Again, such information is held in confidence if it is held subject to an express or implied undertaking to hold it in confidence or it is subject to a restriction on disclosure or an obligation of confidentiality contained in existing legislation. Where the intention is to acquire confidential personal information, or communications of a Member of Parliament, the reasons should be clearly documented and the specific necessity and proportionality of doing so should be carefully considered by the authorising officer in accordance with the safeguards.

20.1.1 Material which has been identified as confidential personal or confidential constituent information should be retained only where it is necessary and proportionate to do so in accordance with the authorised purpose as set out in 9.5 above or where otherwise required by law. It should be securely destroyed when its retention is no longer needed for those purposes. If such information is retained, there should be adequate information management systems in place to ensure that continued retention remains necessary and proportionate for the authorised purpose and the material is marked as confidential. In any case where confidential personal or constituent information is retained, other than for the purpose of destruction, and

disseminated it must be reported to the IPC as soon as reasonably practicable, and any material which has been retained will be made available to the Commissioner on request so that the Commissioner can consider whether the correct procedures and considerations have been applied. Further guidance is detailed within the Home Office Codes of Practice and advice should be sought from the RIPA Co-ordinating Officer.

20.2 **Confidential Journalistic Material**

Confidential journalistic material includes material acquired or created for the purposes of journalism and held subject to an undertaking to hold it in confidence, as well as communications resulting in information being acquired for the purposes of journalism and held subject to such an undertaking. An authorisation to obtain such material will only be granted where the Court are satisfied that there are appropriate safeguards relating to the handling, retention, use and disclosure of the material are in place. Where confidential journalistic material, or that which identifies a source of journalistic information, has been obtained and retained, other than for the purposes of destruction, the matter should be reported to the Commissioner as soon as reasonably practicable by the RIPA Co-ordinating Officer. Further guidance is detailed in the Code of Practice and advice should be sought from the RIPA Co-ordinating Officer.

20.3 **Items subject to Legal Privilege**

Any communication or items held between lawyer and client, or between a lawyer and another person for the purpose of actual or contemplated litigation (whether civil or criminal), must be presumed to be privileged unless the contrary is established: for example, where it is plain that the communication or item does not form part of a professional consultation of the lawyer, or there is clear evidence that the 'furthering a criminal purpose' exemption applies. Where there is doubt as to whether the material is subject to legal privilege or over whether material is not subject to legal privilege due to the "in furtherance of a criminal purpose" exception, advice should be sought from a the RIPA Co-ordinating Officer. The acquisition of matters subject to legal privilege is particularly sensitive and may give rise to issues under Article 6 (right to a fair trial) of the ECHR as well as engaging Article 8. Further guidance is detailed in the Home Office Code of Practice where it is likely that covert surveillance will result in the acquisition of knowledge of matters subject to legal privilege and advice should be sought from the RIPA Co-ordinating Officer. Where items identified by a Doncaster Council's Legal Services as being legally privileged have been acquired, this should be reported to the Commissioner as soon as reasonably practicable by the RIPA Co-ordinating Officer. Further guidance is detailed in the Code of Practice and advice should be sought from the RIPA Co-ordinating Officer.

20.3.1 **Dissemination**

In the course of an investigation, Doncaster Council must not act on or further disseminate legally privileged items unless it has first informed the IPC that the items have been obtained, except in urgent circumstances. Where there is an urgent need to take action and it is not reasonably practicable to inform the IPC that the material has been obtained before taking action, Doncaster Council may take action before informing the IPC and in consultation with the Co-ordinating Officer and Senior Responsible Officer in Legal Services. Doncaster Council must not disseminate privileged items if doing so would be contrary to a condition imposed by the IPC in relation to those items. The dissemination of legally privileged material to an outside body should be accompanied by a clear warning that it is subject to legal privilege. It should be safeguarded by taking reasonable steps to remove the risk of it becoming available, or its contents becoming known, to any person whose possession of it might prejudice any criminal or civil proceedings to which the information relates, including law enforcement authorities. In this regard civil proceedings includes all legal proceedings before courts and tribunals that are not criminal in nature. Legal Services will ensure that the prosecuting authority lawyer who has conduct of a prosecution will not have sight of any legally privileged material, held by the relevant public authority, with any possible connection to the proceedings. In respect of civil proceedings, there can be no circumstances under which it is proper for any public authority to have sight of or seek to rely on legally privileged material in order to gain a litigation advantage over another party in legal proceedings. In order to safeguard against any risk of prejudice or accusation of abuse of process, Doncaster Council will take all reasonable steps to ensure that lawyers or other officials with conduct of legal proceedings should not see legally privileged material relating to those proceedings (whether the privilege is that of the other party to those proceedings or that of a third party). If such circumstances do arise, Doncaster Council will seek independent advice from Counsel and, if there is assessed to be a risk that sight of such material could yield a litigation advantage, the direction of the Court must be sought.

21. Monitoring

21.1 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.

21.2 At least annually the Council's arrangements will be reviewed and a report submitted to the Audit Committee to set the RIPA Policy/Procedures. Interim Update reports shall be delivered to the Committee at intervals of approximately six months.

22. Training and Training Records

22.1 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.

22.2 The Directors shall ensure that appropriate records of such training is retained so that it may be produced during an inspection by the IPC.

23. Working in conjunction with Other Agencies

23.1 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.

23.2 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 RIPA Co-ordinating Officer/Senior Responsible Officer in 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; and

(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.

23.3 In terms of paragraph 23.2(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.

23.4 IF THERE IS ANY REASON FOR DOUBT OR UNCERTAINTY REGARDING PROCEDURAL ISSUES, please consult with the Assistant Director of Legal & Democratic Services or RIPA Co-ordinating Officer at the earliest opportunity.

24. 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 General Data Protection Regulations, Data Protection Act 2018 and the Codes of Practice and relevant DMBC policies.

25. Internal Overview, Equipment and Records Management

25.1 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* Codes 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 IPC. The Assistant Director regularly attends Corporate Leadership Team meetings in accordance with the requirements of the *RIPA* Codes of Practice.

25.2 **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 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**.**

25.3 **Councillor Overview Role**

The Codes also require that:

a) Councillors should review the use of *RIPA* by DMBC and also review and set the policy/procedures 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.

25.4 **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.

25.5 **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).

25.6 **Central Register maintained by the Assistant Director of Legal & Democratic Services**

Authorised Officers MUST forward each original authorisation form and then each renewal or cancellation form to the Assistant Director of Legal & Democratic Services (as RIPA Senior Responsible Officer) 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 Assistant Director of Legal & Democratic Services they are sent in sealed envelopes and marked 'Strictly Private and Confidential'. The Assistant Director of Legal & Democratic Services will monitor the same and give appropriate guidance, from time to time, or amend this Document, as necessary.

25.7 DMBC will retain records for a period of at least five years from the ending of the authorisation. The IPC can audit/review DMBC's policies and procedures, and individual authorisations.

25.8 **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 five years from the ending of the authorisation. Documentation should be securely maintained, with limited access, to ensure confidentiality is not breached.

25.9 Each form will have a URN. These are allocated by Legal Services (see chapter 16 above).

25.10 **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 IPC.

26. Errors

26.1 **Relevant Errors**

An error must be reported if it is a "relevant error". This is any error in complying with any requirements that are imposed on the Council by any enactment which are subject to review by a Judicial Commissioner, including the RIPA legislation. Examples of relevant errors occurring would include circumstances where:

• Surveillance or property interference activity has taken place without lawful authority.
• There has been a failure to adhere to the safeguards set out Chapter 19 above, in the relevant statutory provisions and Chapter 9 of the Home Office Code of Practice.

26.2 **Timescale for external report**

Errors can have very significant consequences on an affected individual's rights and all relevant errors made by Doncaster Council must be reported to the IPC when the Council is aware of the error. The Assistant Director (Legal and Democratic Services) must notify the IPC as soon as reasonably practicable, and no later than ten working days (or as agreed with the Commissioner) after it has been established that a relevant error has occurred.

26.3 **Error Reporting Form**

Any errors by Doncaster Council must be reported on the Error Reporting Forms that are available on the Legal & Democratic Services intranet page and sent to the Assistant Director (Legal and Democratic Services) using the Monitoring Officer email box immediately when the error comes to the awareness of a council officer. Where the full facts of the error cannot be ascertained within that time, the Assistant Director (Legal and Democratic Services) will send an initial notification with an estimated timescale for the error being reported in full and an explanation of the steps being undertaken to establish the full facts of the error. When the Council identifies that a relevant error may have occurred, the Council will take steps to confirm the fact of an error as quickly as it is reasonably practicable to do so. Where it is subsequently confirmed that an error has occurred and that error is notified to the Commissioner, the Council will inform the Commissioner of when it was initially identified that an error may have taken place.

26.4 **Full external report**

A full report must be sent to the IPC as soon as reasonably practicable in relation to any relevant error, including details of the error and, where it has not been possible to provide the full report within ten working days (or timescale as agreed with the Commissioner) of establishing the fact of the error, the reasons this is the case. The report will include information on the cause of the error; the amount of surveillance conducted and material obtained or disclosed; any unintended collateral intrusion; any analysis or action taken; whether any material has been retained or destroyed; and a summary of the steps taken to prevent recurrence.

26.5 **Errors made in good faith in reliance on information.**

In addition to the above, errors may arise where an authorisation has been obtained as a result of the Council having been provided with information which later proved to be incorrect due to an error on the part of the person providing the information, but on which the public authority relied in good faith. Whilst these actions do not constitute a relevant error on the part of the Council which acted on the

information, such occurrences should be brought to the attention of the IPC as detailed above.

26.6 **Serious Errors**

Section 231 of the Investigatory Powers Act 2016 states that the IPC must inform a person of any relevant error relating to that person if the Commissioner considers that the error is a serious error and that it is in the public interest for the person concerned to be informed of the error. The Commissioner may not decide that an error is a serious error unless he or she considers that the error has caused significant prejudice or harm to the person concerned. The fact that there has been a breach of a person's Convention rights (within the meaning of the Human Rights Act 1998) is not sufficient by itself for an error to be a serious error. In deciding whether it is in the public interest for the person concerned to be informed of the error, the Commissioner must in particular consider:

- The seriousness of the error and its effect on the person concerned.
- The extent to which disclosing the error would be contrary to the public interest or prejudicial to:

(i) national security;
(ii) the prevention or detection of serious crime;
(iii) the economic well-being of the United Kingdom; or
(iv) the continued discharge of the functions of any of the security and intelligence services. Before making his or her decision, the Commissioner must ask the Council which has made the error to make submissions on the matters concerned. Public authorities must take all such steps as notified to them by the IPC to help identify the subject of a serious error. When informing a person of a serious error, the Commissioner must inform the person of any rights that the person may have to apply to the Investigatory Powers Tribunal, and provide such details of the error as the Commissioner considers to be necessary for the exercise of those rights.

26.7 **Internal Review of Errors Process**

The Senior Responsible Officer will review any errors that have occurred on a six monthly basis prior to the report to Audit Committee and will report on any errors that may have occurred in the time period since the last Committee report. The Pre Audit Report 6 monthly Check Report will normally be completed by the RIPA Coordinator and passed to the Senior Responsible Officer. Any required actions will also be referred to in the Audit Committee report.

27. External Overview

27.1 The IPC 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 IPC.

27.2 It is anticipated that the inspectors will speak to the Assistant Director (Legal and Democratic Services) as Senior Responsible Officer, the RIPA Co-ordinating Officer, and Authorising Officers.

27.3 Inspections can take place unannounced. The IPC will have unfettered access to locations, documentation and information systems as necessary to carry out their full functions and duties. Council officers are required to provide all necessary assistance to the Inspectors.

27.4 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.

27.5 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 earlier in this document); and

(c) proportionate (as defined earlier in this document).

27.6 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.

27.7 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.

27.8 If the correct procedures are not followed, evidence may be disallowed by the courts, there could be an adverse inspection report issued by the IPC, a complaint could be made to the Investigatory Powers Tribunal, 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.

28. Use of covert surveillance outside of RIPA

28.1 *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 that the Council maintains 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.

29. Complaints

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

29.2 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.

29.3 Copies of the RIPA Code of Practice and this 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

8th Amendment - January 2019