Appendix 2

DONCASTER METROPOLITAN BOROUGH COUNCIL

NON-RIPA Authorisation Procedure.

Contents

Appendices

1 .Introduction

1.1 This procedure document has resulted from the change in the law in respect of Directed Surveillance under the Regulation of Investigatory Powers Act 2000 (RIPA) and the Regulation of Investigatory Powers (Directed Surveillance and Covert Human Intelligence Sources) Order 2012. From the 1st November 2012 Directed Surveillance under RIPA only applied to the detection and prevention of a criminal offence that attracts a penalty of 6 months imprisonment or more or are offences involving sale of tobacco and alcohol to underage children. This essentially takes out surveillance of disorder (unless it has 6 months custodial sentence) and most summary offences such as littering, dog fouling, underage sales of fireworks lower level benefit fraud and anti-social behaviour from regulation.

1.2 Enforcement officers can undertake such surveillance but because it is not now regulated by the Office of Surveillance Commissioners the Council should have procedures in place to ensure that we can prove that we have given due consideration to necessity and proportionality, central tenets of European Law and the likely grounds of any challenge that may be received.

1.3 RIPA is there to ensure that certain types of covert surveillance undertaken by public authorities is done in such a way as is human rights compliant. RIPA is permissive legislation. Authorisation under RIPA affords a public authority a defence under Section 27 i.e. the activity is lawful for all purposes. However, failure to obtain an authorisation does not make covert surveillance unlawful. Section 80 of RIPA provides that the Act should not be construed so as to make it unlawful to engage in any conduct of that description which is not otherwise unlawful under this Act and would not be unlawful apart from this Act. Case law confirms that lack of authorisation under RIPA does not necessarily mean that the carrying out of directed surveillance is unlawful. Local authorities will still be able use covert surveillance for such purposes as long as it is necessary and proportionate in accordance with Article 8 of the European Convention on Human Rights (right to privacy).

2. Overview

2.1 The forms to be completed are an amended version of RIPA forms as used by the Home Office. It will be the responsibility of Authorising Officers to ensure that their relevant members of staff are suitably trained so as to afford common mistakes appearing on forms for Directed Surveillance authorisations. A current list of authorising officers is available on the Covert Surveillance page of the intranet. Authorising officers will also ensure that staff who report to them follow this Procedure and do not undertake or carry out any form of surveillance without first obtaining the relevant authorisations in compliance with this document.

2.2 Health and safety: Authorising Officers must also pay particular attention to Health and Safety issues that may be raised by any proposed surveillance activity. Under no circumstances should an Authorising Officer approve any form unless, and until s/he is satisfied that the health and safety of Council employees/agents are suitably addressed

and/or risks minimised, so far as is possible and proportionate to/with the surveillance being proposed. A risk assessment should be undertaken. If an Authorising Officer is in any doubt he should obtain prior guidance on the same from Legal Services.

2.3 Private and confidential information: Consideration must be given prior thought before any applications are authorised, as failure to do so may invalidate the admissibility of any evidence obtained. Furthermore, thought must be given before any forms are signed to the retention and disposal of any material obtained under a surveillance authorisation. Where there is any possibility of private and confidential information being obtained through covert surveillance, the application must be authorised by an Authorised Officer.

2.4 Necessity and proportionality: The Authorising Officer must ensure proper regard is had to necessity and proportionality before any applications are authorised. Stock phrases or cut and paste narrative must be avoided as the use of the same may suggest that insufficient detail and consideration had been given to the particular circumstances of any person likely to be the subject of surveillance. Any equipment to be used in any approved surveillance must also be properly controlled, recorded and maintained for audit purposes. The Human Rights Act requires the Council and organisations working on its behalf, pursuant to Article 8 of the European Convention to respect the private and family life of citizens, his home and his correspondence. The European Convention did not however, make this an absolute right, but a qualified right. Accordingly, in certain circumstances the Council may interfere in the citizen's right mentioned above, if such interference is:-(a) in accordance with the law;(b) necessary; and (c) proportionate

2.5 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. It is essential that that all involved with surveillance comply with this procedure and seek advice from Legal Services.

3.Types of Surveillance

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 devices. Surveillance can be overt or covert.

3.2 Overt Surveillance: Most of the surveillance carried out by the Council will be done overtly – there will be nothing secretive, clandestine or hidden about it. In many cases, officers will be going about Council business openly. Similarly, surveillance will be overt if the subject has been told it will happen (e.g. where a noise maker 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 of 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. It cannot however be necessary if there is reasonably available an overt means of finding out the information desired.

3.4 Directed Surveillance: Directed Surveillance is surveillance which:-is covert; and Is not intrusive surveillance. The Council must not carry out any intrusive surveillance or any interference with private property. It should not carry out any unauthorised surveillance unless 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. Authorisation must be obtained where surveillance 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).

3.5 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 a 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 them and others that they comes into contact, or associates with. Similarly, although overt town centre CCTV cameras do not formally require authorisation, if the cameras are to be directed for a specific purpose to observe particular individuals, authorisation will be required. The way a person runs their business may also reveal information about their private life and the private lives of others.

3.6 Investigations involving Social Media: 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. 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 RIPA authorised, at the minimum, as directed surveillance. If the investigator engages in any form of relationship with the account operator then they become a Covert Human Intelligence Source (CHIS) requiring authorisation as such and management by a Controller and Handler with a record being kept and a risk assessment created. It will only be in

exceptional circumstances that a NON RIPA authorisation will be considered appropriate for social media. 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. Authorisation will be required.
- 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 an authorisation should be obtained.
- Authorisation should also be considered where a friend request is sent or if a conversation has been entered into 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.

3.7 Procedure: For the avoidance of doubt, only those Officers designated and certified to be Authorised Officers for the purpose of surveillance can authorise an application for Directed Surveillance if and only if the authorisation procedures detailed in this document are followed.

3.8 Necessity and Proportionality: Obtaining an authorisation under the non RIPA surveillance procedure will only ensure that there is a justifiable interference with an individual's Article 8 rights if it is necessary and proportionate for these activities to take place. RIPA requires that the person granting an authorisation believe that the authorisation is necessary in the circumstances of the particular case for directed surveillance. Once necessity is established then proportionality must be considered. The following elements of proportionality should be considered: balancing the size and scope of the proposed activity against the gravity and extent of the perceived crime or offence; explaining how and why the methods to be adopted will cause the least possible intrusion on the subject and others; considering whether the activity is an appropriate use of the legislation and a reasonable way, having considered all reasonable alternatives, of obtaining the necessary result; evidencing, as far as reasonably practicable, what other methods had been considered and why they were not implemented. This involves the balancing the intrusiveness of the activity on the target subject and others who might be affected by it or against the need for the activity in operational terms. The activity will not be proportionate if it is excessive in the circumstances – each case will be judged on and be unique on its

merits – or if the information which is sought could be reasonably be obtained by other less intrusive means. All such activity must be carefully managed to meet the objective in question and must not be arbitrary or unfair. Extra care should also be taken over any publication of the product of the surveillance.

3.9 It is important that when setting out the proportionality and necessity of the surveillance, that the applications include clear statements of the other reasonably possible methods of obtaining the desired information and the reasons why they gave been rejected. It is therefore crucial that the Authorising Officer give particular attention to necessity and proportionality and expresses his own view rather than those explanations given by the applicant.

3.10 Collateral Intrusion: Before authorising surveillance the Authorising Officer should also take into account the risk of intrusion into the privacy of persons other than those who are directly the subjects of the investigation or operation (collateral intrusion). Measures should be taken, wherever practicable, to avoid or minimise unnecessary intrusion into the lives of those not directly connected with the investigation or operation. Those carrying out the surveillance should inform the Authorising Officer if the investigation or operation unexpectedly interferes with the privacy of individuals who are not covered by the authorisation. When the original authorisation may not be sufficient, consideration should be given to whether the authorisation needs to be amended and reauthorized or a new authorisation is required.

3.11 Retention and destruction of product surveillance:. Where the product of surveillance could be relevant to pending or future criminal or civil proceedings, it should be retained in accordance with established disclosure requirements for a suitable period and subject to review. There is nothing which prevents material obtained from properly authorised surveillance from being used in other investigations. Authorising Officers must ensure therefore, that they follow the procedures for handling, storage and destruction of material obtained through the use of covert surveillance. Authorising Officers must also ensure compliance with the appropriate data protection requirements.

4 Authorisation Procedures

4.1 Directed Surveillance can only be lawfully carried out if properly authorised, and in strict accordance with the terms of the authorisation.

4.2 Authorising Officers: Forms can only be signed by Authorising Officers. Legal Services will keep the list of Authorising Officers up to-date. All authorisations for Directed surveillance are for specific investigations only, and must be reviewed, renewed or cancelled once the specific surveillance is complete or about to expire. The authorisations do not lapse with time. On completion of the authorisation , the Authorising officer must pass the the authorised form to by Legal Services (using Document 5 in the Appendices) to be

approved. Surveillance cannot commence until written approval has been obtained from Legal Services for the surveillance.

4.3 Training Appropriate training has been given to Authorising Officers and Enforcement personnel. The training is an ongoing programme and an online course is available on the intranet.

4.4 Application Forms: Only the surveillance forms set out in this document and available on the Councils intranet are permitted to be used. Any other forms used will be rejected by the Authorising Officer and/or Legal Services. The forms are

1. Non RIPA Application for Authorisation to carry out Directed Surveillance
2. Non RIPA Review of a Directed Surveillance Authorisation
3. Non RIPA Renewal of a Directed Surveillance Authorisation
4. Non RIPA cancellation of Directed Surveillance Authorisation
5. NON – RIPA form for legal services approval

4.5 Grounds for Authorisation: Directed Surveillance which does not meet the crime threshold under RIPA has no statutory grounds. However, the Council will only authorise on the grounds of preventing or detecting crime or disorder.

4.6 Assessing the Application Form: Before an Authorising Officer signs a form, they must:- (a) Follow the procedures as laid down in this procedure (b) Satisfy themselves that an authorisation is:-(i) In accordance with the law (ii) Necessary in the circumstances of the particular case on the grounds mentioned in paragraph (enter) above; and (iii) Proportionate to what it seeks to achieve.

4.7 In assessing whether or not the proposed surveillance is proportionate the Authorising Officer must consider whether there are any other non-intrusive means to meet the required aim, if there are none, whether the proposed surveillance is no more than necessary to achieve the objective, as the least intrusive method will be considered proportionate by the Courts. Consideration is required of the risk of intrusion into the privacy of persons other than the specified subject of the surveillance (Collateral intrusion). Measures must be taken wherever practicable to avoid or minimise (so far as is possible) collateral intrusion as the matter may be an aspect of determining proportionality.

4.8 Completing the Application Form: All forms must be given a unique reference number. Legal Services will issue the unique reference number. A date for review of the authorisation should be set. The review should take place on that date using the relevant form. A copy of every form/notice and documents in support must be sent to Legal Services for the Central Register within one week of the relevant authorisation, review, renewal, cancellation or rejection.

4.9 Duration: There is now no specified time for duration but it is proposed to keep to the times provided for under RIPA for consistency. Forms must be reviewed in the time stated, renewed and/or cancelled once it is no longer needed. The authorisation to carry out/conduct the surveillance lasts for a maximum of three months (from authorisation) for Directed Surveillance. In other words the forms do not expire, they have to be reviewed, renewed and/or cancelled once they are no longer required. Authorisations should be renewed before the maximum period in the authorisation 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. An authorisation cannot be renewed after it has expired. In such event a fresh authorisation will be necessary.

4.10 Record Management: A Central Register of all Authorisations, Reviews, Renewals and Cancellations and Rejections will be maintained and monitored by Legal Services in regard to Non RIPA Directed Surveillance. Authorised Officers will be required to send Legal Services a copy of all forms with immediate effect – within one week of authorisation. The Council will retain records for a period of at least three years from the ending of the authorisation. The documents to be stored will include a copy of the Forms together with any supplementary documentation and notification of the approval given by the Authorising Officer

4.11 Risks: . Where there is an interference with the right to respect for private life and family guaranteed under Article 8 of the European Convention on Human Rights, and where there is no other source of lawful authority for the interference, or if it is held not to be necessary or proportionate to the circumstances, the consequences of not obtaining or following the correct authorisation procedure set out in this document, may be that the action (and the evidence obtained) will be held to be unlawful by the Courts pursuant to Section 6 of the Human Rights Act 1998. Challenges could also occur under Article 8 of the European Convention on Human Rights. Obtaining an authorisation and following this document, will assist in showing that the action is carried out in accordance with the law and subject to stringent safeguards against abuse of anyone's human rights.

Policy drafted: November 2017

Appendices

1. Non RIPA Application for Authorisation to carry out Directed Surveillance

2. Non RIPA Review of a Directed Surveillance Authorisation

3. Non RIPA Renewal of a Directed Surveillance Authorisation

4. Non RIPA cancellation of Directed Surveillance Authorisation

5.NON – RIPA form for legal services approval