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 Investigatory Powers Commissioner's Office (IPC). 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: 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. 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). Special considerations apply where any confidential information has been obtained and it may be necessary to notify the Investigatory Powers Commissioner. If such information is obtained you must immediately contact the RIPA Co-ordinating 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 by the Investigatory Powers Tribunal. 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 (see the definition below). 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 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.

3.7 Investigations involving Social Media: The internet provides 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. 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 cover surveillance authorisation. But where a public authority is systematically collecting and recording information about a particular person or group, an 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. Officers should not engage in any form of relationship with the account holder. 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.

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 an 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.

Where covert surveillance using the internet is being considered the 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.

It will only be in exceptional circumstances that a NON RIPA authorisation will be considered appropriate for social media. Before any such investigation commences, the Assistant Director, Legal and Democratic Services should be contacted. Further guidance is also available on the intranet in the Council's RIPA procedure.

3.8. 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 Covert Surveillance Code of Practice should be considered as to whether a covert 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. Before any such investigation commences, the Assistant Director, Legal and Democratic Services should be contacted.

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

3.10 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 believes 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.

3.11 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.

3.12 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.

3.13 Safeguards and 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. 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.

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. 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. Dissemination, copying and retention of material must be limited to the minimum necessary for authorised purposes. Further information on the use of information as evidence, handling and dissemination of materials, coping, storage and destruction is detailed in the RIPA procedure.

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 authorised form to 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 or for the purposes of safeguarding children or vulnerable adults.

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 immediately 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 and compensation may be payable to those whose privacy rights have been infringed. 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.

5. Errors

An error must be reported to the IPC if it is a "relevant error". This is any error in complying with any requirements that are imposed on it 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 in the relevant statutory provisions and Chapter 9 of the Statutory Code of practice.

For the purposes of this procedure, it may be where covert surveillance has taken place without following this procedure where it should have been.

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. Therefore, where an officer becomes error of an error, they must immediately notify the Assistant Director of Legal and democratic Services. Further detailed information is available on this in the Chapter 26 of the Council's RIPA procedure.

Policy drafted: November 2017

Updated: January 2019

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