

**POLICY AND PROCEDURES  
FOR  
UNDERTAKING SURVEILLANCE NOT COVERED BY THE  
REGULATION OF INVESTIGATORY POWERS ACT 2000**

**EFFECTIVE AS FROM  
1 NOVEMBER 2015 (UPDATED Oct 2017)**

**NON - RIPA**

## Contents

		<b>Page Number</b>
1.0	Introduction	3
2.0	General Information on Human Rights	3
3.0	Types of Surveillance	5
4.0	Authorisation Procedures	8

Date last Reviewed October 2017

Version No            2

Review date            September 2018

## **1.0 Introduction**

- 1.1. This policy and 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.
- 1.2. RIPA does not grant powers to carry out surveillance. It simply provides a framework that allows the Council to authorise and supervise surveillance in a manner that ensures compliance with the Human Rights Act 1998. Equally RIPA does not prevent surveillance from being carried out or require that surveillance may only be carried out under RIPA
- 1.3. Directed Surveillance under RIPA will only apply to the detection and prevention of a criminal offence that attracts a penalty of 6 months imprisonment or more. The Council has a separate policy and procedure for undertaking covert surveillance and use of covert human intelligence sources in accordance with RIPA where the offence will attract a penalty of more than 6 months.
- 1.4. There may be times when it will be necessary to carry out covert Directed Surveillance or use a CHIS other than by using RIPA. For example, in relation to an investigation that a member of staff or a contractor is not carrying out their work as contracted, then a RIPA authorisation is not usually available in such circumstances, because criminal proceedings are not normally contemplated
- 1.5. Also this means that RIPA regulations do not apply in most cases where the Council suspects a summary offence has been committed for example littering, dog fouling, and anti-social behaviour.
- 1.6. Adherence to this policy enables the Council to show that consideration has been given to the necessity and proportionality of surveillance activity.

## **2.0 General information on Human Rights**

- 2.1. 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
- 2.2. 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. All employees involved with surveillance comply with this document and

any further guidance that may be issued from time to time by Legal Services.

- 2.3. Staff should not undertake any form of surveillance without first obtaining the relevant authorisations in compliance with this document.
- 2.4. 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 is 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 s/he should obtain guidance from Legal Services.
- 2.5. Coming across private and confidential information<sup>1</sup> during surveillance 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 the Chief Executive or in his absence an Executive Director (see Policy and Procedures for Undertaking Surveillance and Use of Covert Human Intelligence Sources)
- 2.6. When completing forms standard phrases or cut and paste narrative must be avoided as this can suggest that insufficient consideration has been given to the particular circumstances of the request. Any equipment to be used in any approved surveillance must also be properly controlled, recorded and maintained for audit purposes.

### **Types of Surveillance**

- 3.1. Surveillance can be overt or covert and includes:
  - Monitoring, observing, listening to persons, watching or following their movements, listening to their conversations and other such activities or communications;
  - Recording anything mentioned above in the course of authorised surveillance;
  - Surveillance, by or with, the assistance of appropriate surveillance device(s);

---

<sup>1</sup> Confidential personal information is information held in confidence relating to the physical or mental health or spiritual counselling concerning an individual (whether living or dead) who can be identified from it. By its very nature, where such information is likely to be acquired, then authorisation is required from either the Chief Executive or in his absence an Executive Director, see Policy and Procedures for Undertaking Surveillance and Use of Covert Human Intelligence Sources

### **Overt Surveillance**

- 3.2. Much 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.
- 3.3. Similarly, surveillance will be overt if the subject has been told it will happen (e.g. where a noise maker is warned that noise will be recorded 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.

### **Covert Surveillance**

- 3.4. Covert surveillance is carried out in a manner calculated to ensure that the person subject to the surveillance is unaware of it taking place.

### **Directed Surveillance**

- 3.5. Directed Surveillance is surveillance which:
  - a. Is covert; and
  - b. Is not intrusive surveillance (see definition below – the Council **must not** carry out any intrusive surveillance or any interference with private property);
  - c. Is not carried out in 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
  - d. 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)
- 3.6. 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 him/her and others that he/she comes into contact, or associates with.
- 3.7. 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 his/her business may also reveal information about his or her private life and the private lives of others.

3.8. 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.

3.9. Intrusive Surveillance cannot be carried out by the Council

### **Tracking Devices – Tracking Rubbish**

3.10. Tracking devices to be used in or on skips can be authorised by Authorising Officers provided that the tracking device is disguised as refuse and is not physically attached/affixed to the skip. In the event of there being a requirement that a vehicle tracking device be used and that to install such a device interfered with property not owned by the Council, authorisation will need to be obtained from the police under the Police Act 1997. In either case officers are required to contact Legal Services before authorisation is given.

### **Necessity and Proportionality**

3.11. Obtaining an authorisation under this policy and 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.

3.12. The following elements of proportionality should be considered:

- balancing the size and scope of the proposed activity against the 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; and
- evidencing, as far as reasonably practicable, what other methods had been considered and why they were not implemented

3.13. This involves 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.

- 3.14. It is important that when setting out the proportionality 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 have been rejected. This approach will apply, equally, to arguments for the necessity of surveillance. It is therefore crucial that the Authorising Officer give particular attention to necessity and proportionality and expresses their own view rather than those explanations given by the applicant.

### **Collateral Intrusion**

- 3.15. 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.
- 3.16. 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 reauthorised or a new authorisation is required.

### **Retention and destruction of product surveillance**

- 3.17. 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.
- 3.18. 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.

## **4.0 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.

### **Authorising Officers**

- 4.2 Forms can only be signed by Authorising Officers.
- 4.3 Authorisations are separate from delegated authority to act under the Council's scheme of delegation and internal departmental schemes of delegation. 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.

### **Application Forms**

- 4.4 In the circumstances outlined above, a RIPA application may be completed in accordance with this Policy and the application must be clearly endorsed in red "NON-RIPA SURVEILLANCE" along the top of the first page. The application must be submitted in the normal fashion to the Authorising Officer who must consider it under the necessity and proportionality test in the same way they would a RIPA application

### **Assessing the Application Form**

- 4.5 Before an Authorising Officer signs a form, s/he must:
- a. Follow the procedures as laid down in this policy. If you are in any doubt please contact Legal Services
  - 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.
  - c. In assessing whether or not the proposed surveillance is proportionate 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.**
- 4.6 Take into account 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.

### **Duration**

- 4.7 There is no specified time for the duration of non-RIPA surveillance, but the Council will adhere to the time frames outlined in 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.
- 4.8 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.

### **Record Management**

- 4.9 A Central Register of all Authorisations, Reviews, Renewals and Cancellations and Rejections will be maintained and in regard to Non RIPA Directed Surveillance. Authorised Officers will be required to send a copy of all forms to the Councils A-FACT Manager – within one week of authorisation.
- 4.10 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;
  - A record of the period over which the surveillance has taken place;
  - The frequency of reviews prescribed by the Authorising Officer;
  - A record of the result of each review of the authorisation
  - A copy of any renewal of any authorisation, together with the supporting documentation submitted when the renewal was requested; and
  - The date and time when any instruction was given by the Authorising Officer.