

# **OXFORD CITY COUNCIL**

## **Regulation of Investigatory Powers Act 2000**

### **Policy and Procedure**

**OXFORD CITY COUNCIL  
LAW AND GOVERNANCE**

**May 2018**

## **1. INTRODUCTION**

- 1.1 Any covert surveillance conducted by the Council can constitute an interference with the right protected by Article 8 of the European Convention on Human Rights, which provides that every individual has a “right to respect for his private and family life, his home and his correspondence”. Section 6 of the Human Rights Act 1998 provides that it is unlawful for the Council to interfere with those rights unless it is in accordance with the law, proportionate and necessary in a democratic society.
- 1.2 As the Council has a number of functions to undertake which involve the enforcement of laws and regulations, officers will need to conduct investigations and where appropriate take legal proceedings. The Council will not normally make use of covert surveillance and similar activities unless it is necessary for an investigation and it is seen as a last resort. The covert surveillance method requested must also be the least intrusive available.
- 1.3 The Regulation of Investigatory Powers Act 2000 (RIPA) regulates the way in which the Council conducts surveillance for the purposes of law enforcement. The fundamental requirement of RIPA is that when the Council considers undertaking directed surveillance or using a covert human intelligence source it must only do so if:
  - a) the activity has been authorised by an officer with appropriate powers, and
  - b) the relevant criteria are satisfied and that the alleged offences carry a minimum sentence of six months imprisonment (or is a statutory exception see para 3.4) and that confirmation of approval has been given by a Magistrate.
- 1.4 Some activities of Council enforcement officers (e.g. environmental health officers, benefit fraud investigators, planning enforcement officers, licensing officers) are covered by the provisions of this Act. Also covered by the Act and less obviously, are activities, which involve surveillance for purposes, which, might be said to be internally focussed.
- 1.5 Compliance with RIPA will ensure any interference is in accordance with domestic law. Compliance with RIPA assists to defend complaints against the Council and officers of interference with the right to respect for private and family life protected by Article 8 of the Convention. The Council can thus claim any interference is “in accordance with the law”. Provided the activities undertaken are also necessary and proportionate there will be no contravention of human rights legislation.

- 1.6 All investigations or enforcement actions involving covert surveillance or the use of a covert human intelligence source must comply with the provisions of RIPA.
- 1.7 This policy applies to all staff and agents working for the Council. The purpose of this guidance is to advise Council enforcement officers and their managers of the procedure that should be followed where surveillance activities are contemplated, to ensure compliance with RIPA.
- 1.8 The Council will from time to time issue further guidance and procedures to staff.
- 1.9 The Council will ensure adequate training takes place for authorising and investigating officers.
- 1.10 This policy should be read in conjunction with the Regulation of investigatory Powers Act 2000 (RIPA) and the Home Office Codes of Practice 2014, and for further guidance see Office of Surveillance Commissioners Procedures and Guidance 2016\*.

<https://www.gov.uk/government/publications/covert-surveillance-and-covert-human-intelligence-sources-codes-of-practice>,

\* *The Investigatory Powers Commissioners Office (IPCO) is reviewing the content for the previous oversight bodies websites with a view of consolidating the contents on to its new website. In the meantime please contact the RIPA Coordinating Officer for a copy of the 2016 Procedures and Guidance.*

## **2. RIPA REGULATED ACTIVITIES**

- 2.1 If an investigating officer identifies a contemplated surveillance activity as regulated by RIPA, a written authorisation in accordance with this guidance should be obtained, before the activity commences. If enforcement officers or their managers are in any doubt, they should contact the Head of Law & Governance.

Activities covered by RIPA:

### **2.2 The Interception of Communications**

Where interception of the communication has not been authorised, or agreed by the sender and addressee of the communication. These guidance notes do not cover this activity, as the Council is extremely unlikely to undertake this activity. Please contact the Head of Law & Governance.

## 2.3 The Use of Covert Human Intelligence Sources

This is defined as the use of an individual to create a relationship with a subject, for the purposes of obtaining information, where the purpose of the relationship is not disclosed to the subject. Interaction with the subject of surveillance is therefore required in order for an individual to be regarded as a covert human intelligence source (CHIS). Activities of an undercover officer could fall within this definition. Additional careful monitoring and recording is required (see Home Office Code of Practice *CHIS* chapter 6).

2.3.1 Examples might include an undercover police officer who, attempts to infiltrate a drug smuggling ring. Another example might be the use of a professional witness or private investigator to obtain information and evidence where that individual interacts with the subject of surveillance.

2.3.2 Members of the public who volunteer information as part of their civic duty i.e. they voluntarily disclose to the Council observations which they have made during the course of their lives, will not normally be regarded as a CHIS. It will be otherwise if they have obtained the information in the course of a friendship or other relationship with the suspect. In case of any doubt, legal advice should be sought from the Head of Law and Governance.

2.3.3 The Council does not envisage any circumstances where it would be necessary to use a CHIS. An authorising officer must consult with the Head of Law & Governance before considering authorising the use of CHIS.

## 2.4 Directed Surveillance

As this activity is the most likely to be carried out, this policy addresses this activity in more detail. Where there is to be directed surveillance written authorisation must be obtained in accordance with the provisions of RIPA before the surveillance commences. Directed surveillance is defined as surveillance which is covert, but not intrusive and which is undertaken for the purposes of a specific investigation, and which is likely to result in obtaining private information about a person and which is carried out otherwise than as an immediate response to events where it would be impracticable to obtain prior authorisation.

2.4.1 Therefore investigating officers need to consider a number of key questions to determine whether a proposed activity falls within this definition of directed surveillance:

- i) **Is the proposed activity surveillance?**

Surveillance is defined in wide terms as: any activity involving the monitoring, observing or listening to persons, their movements, their conversations or other activities or communications; the recording of anything monitored, observed or listened to in the course of surveillance; and the surveillance by or with the assistance of a surveillance device.

- ii) **Is the surveillance covert?**  
Surveillance is covert where it is carried out in a manner calculated to ensure that the subjects of the surveillance are unaware that it is, or may be taking place. It is therefore the intention of the officer carrying out the surveillance, which is relevant to this issue of covertness.
- iii) **Is the surveillance for the purposes of a specific investigation?**  
General observation, not forming part of any investigation into suspected breaches of the law and not directed against any specific person or persons is not directed surveillance e.g. CCTV cameras in Council car parks are readily visible and if they are used to monitor the general activities of what is happening within the car park, it falls outside the definition. If, however, the cameras are targeting a particular known individual, the usage will become a specific operation, which will require authorisation.
- iv) **Is the surveillance undertaken in such a manner that is likely to result in the obtaining of private information about a person?**  
“Private Information” is any information concerning a person’s private or family life. Whether information is personal in nature is relevant when deciding whether information is private. The fact that observation of individuals occurs from the public highway will not prevent the discovery of private information. When officers consider this question they should give due weight to the probability of discovering such information, as authorisation is not required if there is only a slight possibility of discovering private information.
- v) **Is the surveillance otherwise than by way of an immediate response to events or circumstances where it is not reasonably practicable to obtain prior authorisation?**  
If the surveillance were an immediate response to something happening during the course of an officer’s work, it would not be reasonable to obtain prior authority. If this occurs, the officer must report the incident back to

an authorising officer so a note can be made on the relevant department file and the central register.

vi) **Is the surveillance intrusive?**

The Council is not authorised to carry out intrusive surveillance however it is extremely unlikely the Council would contemplate undertaking this activity. Directed surveillance turns into intrusive surveillance if it is carried out in relation to anything taking place on residential premises or in a private vehicle, and involves the presence of an individual on the premises or in the vehicle. If a surveillance device is used and if the device is not on the premises or in the vehicle, it is only intrusive if it consistently produces information of the same quality as if it were. To be approved the Authorising Officer must be satisfied that necessity, proportionality and collateral intrusion have all been properly addressed (see Home Office Code on Convert Surveillance chapter 3).

3. **AUTHORISATIION**

- 3.1 An application for the carrying out of directed surveillance or the use of a CHIS must first be given independent consideration by an Authorising Officer who will give written reasons for approval. The complete application must then be taken to the Magistrates' Court where after a hearing; confirmation of the appropriateness of the action must be obtained from the Magistrate.
- 3.2 The contact numbers for the Oxford Magistrates' Court are 448021 or 448032.
- 3.3 A copy of the Home Office guidance to local authorities and a copy of the application for judicial approval can be obtained at <http://www.homeoffice.gov.uk/publications/counter-terrorism/ripa-forms/local-authority-ripa-guidance>
- 3.4 In addition to obtaining prior judicial approval an authorisation for directed surveillance or the use of a CHIS can only be granted if the offence under investigation carries a maximum term of imprisonment of at least 6 months whether at the Magistrates' Court or the Crown Court, or would constitute an offence of:
  - a) selling alcohol to children contrary to section 146 of the Licensing Act 2003;
  - b) allowing the sale of alcohol to children contrary to section 147 of the Licensing Act 2003;
  - c) persistently selling alcohol to children contrary to section 147A of the Licensing Act 2003; or,

- d) the sale of tobacco etc. to persons under 18 contrary to section 7 of the Children and Young Persons Act 1933.

#### 4. **AUTHORISING OFFICERS**

- 4.1 The Regulation of Investigatory Powers (Directed Surveillance and Covert Human Intelligence Sources) Order 2003 No. 3171 prescribes the authorising officer must be at least an Assistant Chief Officer, Assistant Head of Service, Service Manager or equivalent.
- 4.2 The Council's authorising officers are The Chief Executive, The Executive Director for Community Services, The Head of Law & Governance and The Head of Finance. It should be noted that the Head of Law & Governance is also the Senior Responsible Officer (SRO) for the purposes of RIPA. It is generally undesirable for an SRO to act as an authorising officer. Authorisation from the Head of Law & Governance should only be sought in the event that the other authorising officers are unavailable.
- 4.3 Authorising officers should not be responsible for authorising investigations or operations in which they are directly involved, although it is recognised that this may sometimes be unavoidable in cases where it is necessary to act urgently. Where an authorising officer authorises such an investigation or operation a note of the authorisation should be placed on the central record of authorisations (see paragraph 8.3).
- 4.4 Authorising officers must be aware of the requirements of RIPA and how to properly consider requests for authority. Authorising officers must demonstrate that these requests have been properly considered when they complete the authorisation form.
- 4.5 Where the surveillance is likely to lead to the obtaining of confidential information, a RIPA authorisation can only be given by The Chief Executive or the person acting as such in his/her absence. In these circumstances the power to issue RIPA authorisations cannot be delegated. For these purposes confidential information is:
  - (a) legally privileged information e.g. communications between a professional legal adviser and a client
  - (b) confidential personal information, which is information kept in confidence and relating to a person's physical or mental health or relating to spiritual counselling given to a person e.g. consultations between a health professional and a patient, information from a patient's medical records or conversations between an individual and a Minister of Religion

(c) confidential journalistic information, which is any information, held for the purposes of journalism on the basis that it or its source would not be revealed.

- 4.6 If any such information is obtained during surveillance legal advice should be sought immediately.
- 4.7 Chapter 3 of both Codes of Practice referred to at paragraph 9.1 below provide further guidance relating to confidential material.

## 5. **FORMS OF AUTHORITY**

- 5.1 The Act does not contain prescribed forms of authority. The Home Office model forms should be used. This will ensure a consistent approach is adopted across the Council and ensure all relevant issues are addressed during the decision-making process. Forms relating to directed surveillance and the use of covert human intelligence sources are available from the Home Office at <http://www.gov.uk/government/collections/ripa-forms--2>

## 6. **DURATION OF AUTHORISATIONS**

- 6.1 A written authorisation for directed surveillance lapses, if not renewed, three months from the grant or last renewal. Officers should ensure authorisations only last for as long as is considered necessary and proportionate. Regular reviews of authorisations should be undertaken to assess the need for continued surveillance.
- 6.2 Any time before the authorisation would cease to have effect, the authorising officer may renew, in writing, if he/she still considers it necessary and proportionate.
- 6.3 Authorisations may be renewed more than once provided they continue to meet the criteria for authorisation. The renewal does not have to be authorised by the same authorising officer who granted the original authorisation.
- 6.4 The authorising officer who granted the authorisation or last renewed the authorisation must cancel it if he is satisfied the directed surveillance no longer meets the criteria upon which it was authorised.

## 7. **COVERT SURVEILLANCE OF SOCIAL NETWORKING SITES (SNS)**

- 7.1 The fact that digital investigation is routine or easy to conduct does not reduce the need for authorisation. Care must be taken to understand how the SNS being used works. Authorising Officers must not be tempted to assume that one service provider is the same as another



or that the services provided by a single provider are the same.

- 7.2 Whilst it is the responsibility of an individual to set privacy settings to protect unsolicited access to private information, and even though data may be deemed published and no longer under the control of the author, it is unwise to regard it as “open source” or publicly available; the author has a reasonable expectation of privacy if access controls are applied. In some cases data may be deemed private communication still in transmission (instant messages for example). Where privacy settings are available but not applied the data may be considered open source and an authorisation is not usually required. Repeat viewing of “open source” sites may constitute directed surveillance on a case by case basis and this should be borne in mind.
- 7.3 Providing there is no warrant authorising interception in accordance with section 48(4) of RIPA, if it is necessary and proportionate for a public authority to breach covertly access controls, the minimum requirement is an authorisation for directed surveillance. An authorisation for the use and conduct of a CHIS is necessary if a relationship is established or maintained by a member of a public authority or by a person acting on its behalf (i.e. the activity is more than mere reading of the site’s content).
- 7.4 It is not unlawful for a member of a public authority to set up a false identity but it is inadvisable for a member of a public authority to do so for a covert purpose without an authorisation for directed surveillance when private information is likely to be obtained. The SRO should be satisfied that there is a process in place to ensure compliance with the legislation. Using photographs of other persons without their permission to support the false identity infringes other laws.
- 7.5 A member of a public authority should not adopt the identity of a person known, or likely to be known, to the subject of interest or users of the site without authorisation, and without the consent of the person whose identity is used, and without considering the protection of that person. The consent must be explicit (i.e. the person from whom consent is sought must agree (preferably in writing) what is and is not to be

## 8. **RETENTION AND SECURITY OF FORMS AND RECORDS**

- 8.1 Requests for authorisations, renewals, cancellations are confidential material. The documents and any information contained therein must not be disclosed to any person who has no legitimate need to have access to the document, or to the information that it contains. Authorising Officers must ensure that there are proper arrangements within their departments or services for the retention and security of such documents.
- 8.2 Such documents may need to be securely kept for a period (considered appropriate by the relevant Head of Service) following the completion of

any surveillance, as they may have to be produced in Court, or to the other party in Court proceedings as part of legal disclosure requirements. Superfluous copies should not be made or kept.

- 8.3 The Head of Law & Governance maintains a central register of all authorisations, reviews, cancellations and renewals. Authorising officers should ensure that hard copies of these documents are sent to the Head of Law & Governance as soon as is practicable.
- 8.4 The central register will be “weeded” of information that is more than six years old, unless there are relevant outstanding Court proceedings. All documentation that is no longer needed will be shredded.

## 9. **CODES OF PRACTICE**

- 9.1 The Covert Surveillance [Code of Practice](#).
- 9.2 The Code of Practice is admissible as evidence in criminal and civil proceedings. The Council will follow the requirements of any Codes of Practice issued by the Home Secretary unless there are exceptional circumstances justifying a departure from the recommended approach.

## 10 **RIPA OFFICERS**

- 10.1 The Senior Responsible Officer at Oxford City Council is Anita Bradley, Head of Law & Governance.
- 10.2 The RIPA Coordinating Officer at Oxford City Council is Jeremy Franklin.

Anita Bradley  
Senior Responsible Officer  
Head of Law & Governance  
Oxford City Council