ADUR & WORTHING
COUNCILS

**Joint Governance Committee**
**26 September 2017**
**Agenda Item 13**

**Ward:** All

**The Councils' Surveillance Powers, Policy and Procedures**

**Report by the Solicitor to the Councils & Monitoring Officer**

## 1.0 Summary

1.1 To agree a revised joint Surveillance Policy and Procedure to ensure compliance with the Regulation of Investigatory Powers Act 2000 and to note the Councils' use of those powers.

## 2.0 Background

2.1 The Regulation of Investigatory Powers Act 2000, as amended, provides a scheme whereby surveillance can be carried out by the Councils, in accordance with an authorisation granted under the Act, and the appropriate judicial approval, and that such surveillance shall be lawful for all purposes. Failure with compliance with the statutory framework could lead to evidence obtained by way of surveillance being inadmissible in Court and/or the Councils facing civil or criminal action for breach of statutory or common law rules relating to the privacy of individuals.

2.2 The surveillance must be necessary for the purpose of preventing or detecting conduct which constitutes a criminal offence which is punishable by a maximum sentence of a prison term of at least 6 months, or relates to the investigation into alleged underage sales of alcohol and/or tobacco.

2.3 An authorisation may be given for directed surveillance which is:

- for the purposes of a specific investigation,
- covert rather than overt, and
- is likely to result in the obtaining of private information about a person.

An authorisation is not generally required for general observations, drive bys or attendance at trouble hot spots, nor for overt surveillance such as CCTV systems where notice is given to the public, nor for cases where an immediate response is necessary to an occurrence.

Authorisations will, in some circumstances, be required when social media is used in investigations and either the Council breaches privacy controls, there is repeated or targeted monitoring of an individual's social media profile, or a covert human intelligence source (CHIS) is used to interact and communicate with an individual through social media.

2.4 An authorisation may also be given for the use of a covert human intelligence source, whereby a person covertly uses an existing or newly established relationship with an individual in order to provide information to the Council.

2.5 Since the introduction of the Protection of Freedoms Act 2012 an authorisation for directed surveillance or the use of a covert human intelligence source will not take effect until such time as the relevant judicial authority, a Justice of the Peace, has made an order approving the grant of the authorisation.

2.6 Each Council adopted a surveillance policy in 2002 to ensure compliance with the Regulation of Investigatory Powers Act 2000. In 2012 the Councils agreed to adopt a revised single surveillance policy.

2.7 The Councils' policies, practices and procedures are subject to review by the Office of the Surveillance Commissioner and the last inspection was carried out in July 2017. The Commissioner suggested some amendments to the Councils' policy relating in particular to its use of Social Media in investigations, and as such, the proposed Policy and Procedure document has been amended and is attached as Appendix 1 to this report.

2.8 The Home Office Covert Surveillance and Property Interference Code of Practice 2014 paragraph 3.35 states that *"Elected members of a local authority should review the authority's use of the 2000 Act and set the policy at least once a year. They should also consider internal reports on the use of the 2000 Act on a regular basis to ensure that it is being used consistently with the local authority's policy and that the policy remains fit for purpose"*.

2.9 Neither Council has authorised any surveillance under this Policy or the 2000 Act during the financial year 2016/17 nor since. Indeed the powers under the 2000 Act are rarely used by the Councils and when they have been used in the past they were generally in relation to Benefit Fraud investigations, which are now undertaken by the Department of Work and Pensions. Nevertheless, it remains imperative that the Councils have a robust, fit for purpose policy in place, and that Officers involved in investigations and authorising surveillance keep up to date with knowledge and receive regular training.

## 3.0 Proposals

3.1 That the Joint Governance Committee, on behalf of the Councils, approves the Joint Surveillance Policy and Procedure and notes the Councils' use of their powers under the 2000 Act.

## 4.0 Legal

4.1 Sections 26-48 of the Regulation of Investigatory Powers Act, as amended by the Protection of Freedoms Act 2012 and Regulations made under the 2000 Act, sets out the statutory framework for the authorisation of directed surveillance and the use and conduct of covert human intelligence sources.

4.2 Compliance with the Regulation of Investigatory Powers Act 2000 ensures that the Councils and their Officers fulfill the requirements of the Human Rights Act in relation to investigations.

## 5.0 Financial implications

5.1 There are no specific financial implications arising from this report.

## 6.0 Recommendation

6.1 That the Joint Governance Committee agrees the revised Surveillance Policy and Procedure set out in Appendix 1 with immediate effect and notes the Councils' use of their powers under the Regulation of Investigatory Powers Act 2000 as set out in paragraph 2.9 above.

**Local Government Act 1972**
**Background Papers:**

Home Office Covert Surveillance and Property Interference Code of Practice 2014
Office of Surveillance Commissioners Procedures and Guidance 2016
Joint Strategic Committee Report on 'Joint Surveillance Policy and Procedure' dated 26 July 2012

**Contact Officer:**

Susan Sale
Solicitor to the Councils & Monitoring Officer
Town Hall
01903 221119
susan.sale@adur-worthing.gov.uk

## Schedule of Other Matters

### 1.0 Council Priority

1.1 This report does not address any particular Council priority.

### 2.0 Specific Action Plans

2.1 This report does not address any specific action plan.

### 3.0 Sustainability Issues

3.1 This matter does not address any particular sustainability issues.

### 4.0 Equality Issues

4.1 The Policy and Procedure set out within this report provides the opportunity for consideration of equalities issues.

### 5.0 Community Safety Issues (Section 17)

5.1 The Policy and Procedure set out within this report is intended to improve the likelihood for detecting crime, which in itself, should help to reduce crime within the area.

### 6.0 Human Rights Issues

6.1 This Policy and Procedure is intended to ensure that human rights are considered prior to the granting of an authorisation and where authorisation and judicial approval are granted, and surveillance is exercised in accordance with such authorisation and approval, would provide the Councils with protection to any claim that an individual's human rights have been breached.

### 7.0 Reputation

7.1 The Policy and Procedure is intended to ensure that the Councils act properly and proportionately when investigating criminal offences and compliance with an appropriate policy will protect the Councils' reputations as surveillance should only be carried out when necessary, justified and proportionate.

### 8.0 Consultations

8.1 Consultation has been undertaken with the Councils' Leadership Team and the Policy is based upon advice provided by the Office of the Surveillance Commissioner.

### 9.0 Risk Assessment

9.1 Matter considered and no issues identified.

### 10.0 Health & Safety Issues

10.1 Matter considered and no issues identified.

## 11.0 Procurement Strategy

11.1 Matter considered and no issues identified.

## 12.0 Partnership Working

12.1 Matter considered and no issues identified.


ADUR & WORTHING
COUNCILS

**ADUR DISTRICT COUNCIL**

**AND**

**WORTHING BOROUGH COUNCIL**

# SURVEILLANCE POLICY AND PROCEDURE

**September 2017**

# Table of Contents

# PART 1 : POLICY

## 1 INTRODUCTION

1.1 The Councils are each responsible for the enforcement of a wide range of legislation affecting their areas. Such enforcement may have an impact upon individuals, as the Councils gather evidence and decide what action to take in relation to suspected offences. There may be some effect upon the private lives of individuals who may be the subject of surveillance which is unknown to them.

1.2 It is important that such surveillance of individuals and gathering of evidence is carried out in accordance with established legal rules. Also, that it is undertaken only when it is necessary and that the effect on the individuals concerned is taken into account before it goes ahead.

1.3 Failing this, there is a risk that evidence obtained by the Councils may be inadmissible in legal proceedings and/or the Councils may face civil or criminal action for breach of statutory or common law rules relating to the privacy of individuals.

1.4 The Regulation of Investigatory Powers Act 2000 provides a legal framework under which surveillance of individuals for evidence–gathering purposes can be authorised by the Councils. This document sets out a policy for such authorisation (Part I) and associated procedures (Part 2), together with further information on Covert Human Intelligence Sources (Part 3) and a specific section relating to the use of social media in investigations (Part 4).

1.5 The Councils have appointed the Director for Digital and Resources as the Senior Responsible Officer (SRO) for matters relating to the Regulation of Investigatory Powers Act 2000. In accordance with paragraph 3.34 of the Home Office Code of Practice, the Senior Responsible Officer must be a member of the Corporate Leadership Team and is responsible for ensuring that all Authorising Officers are of an appropriate standard in light of any recommendations in the inspection reports prepared by the Office of the Surveillance Commissioner. Where an inspection report highlights concerns about the standards of Authorising Officers, this individual will be responsible for ensuring the concerns are addressed. The Senior Responsible Officer is not an Authorising Officer under RIPA as it is unlikely that he could be regarded as objective if he oversaw his own authorisations.

1.6 The Councils have appointed the Solicitor to the Councils and Monitoring Officer as the RIPA Co-ordinator. The RIPA Co-ordinator shall maintain a central register of all authorisations which will be

retained by the Councils for a period of three years from the ending of any authorisation.

1.7 In accordance with paragraph 3.35 of the Home Office Code of Practice, Elected Members of the Council should review the Authority's use of RIPA and set the Council's Policy, at least once a year. They should also consider internal reports on the use of RIPA on a regular basis, to ensure that it is being used consistently with the Council's Policy and that the Policy remains fit for purpose. The Councils' Joint Governance Committee will consider such matters on an annual basis.

## 2 WHAT IS DIRECTED SURVEILLANCE?

2.1 Surveillance is

(a) monitoring, observing or listening to persons, their movements, their conversations or their other activities or communications,
(b) Recording anything monitored, observed or listened to in the course of surveillance, and
(c) Surveillance by or with the assistance of a surveillance device.

2.2 To be covert surveillance, the surveillance must be carried out in a manner that is calculated to ensure that the persons who are subject to the surveillance are unaware that it is or may be taking place. For example, use of CCTV systems may be overt in many cases, and the public may be made aware of their use. This would be distinct from a case in which CCTV is used covertly for a particular operation and may require authorisation.

2.3 Private information includes any information relating to an individual's private or family life.

2.4 "Directed Surveillance" is surveillance which is:

2.4.1 covert (but not intrusive; see paragraph 3),

2.4.2 conducted for the purposes of a specific investigation or operation, and

2.4.3 is conducted in such a manner as is likely to result in the obtaining of private information about a person (whether or not one specifically identified for the purposes of the investigation or operation).

The planned covert surveillance of a specific person, where not intrusive, would constitute Directed Surveillance if such surveillance is likely to result in the obtaining of private information about that, or any other, person.

For example, if a Council Officer wanted to drive past a café for the purposes of obtaining a photograph of the exterior, no private

information about any person is likely to be obtained or recorded and therefore this is unlikely to amount to Directed Surveillance nor require authorisation. However, if the Council wished to conduct 'drive bys', to establish a pattern of occupancy of the premises by any person, the accumulation of information is likely to result in the obtaining of private information about that person and a Directed Surveillance authorisation should be considered.

2.5 Directed Surveillance does not extend to those cases where an immediate response is necessary to an occurrence and it would not be reasonably practicable to obtain an authorisation (e.g. due to the time involved in obtaining an authorisation).

2.6 General observations undertaken and not linked to any specific investigation would fall outside the definition of Directed Surveillance. Such observations may involve the use of equipment to merely reinforce normal sensory perception, such as the use of binoculars or cameras when this does not involve the systematic surveillance of individuals. For example, routine patrols and observation at trouble 'hotspots' would not constitute Directed Surveillance and would not require authorisation.

2.7 Occasionally, the Councils may authorise the gathering of information by the use of Covert Human Intelligence Sources (CHIS). This is where a person covertly uses an existing or newly-established relationship with an individual in order to provide information to the Council. The purpose behind the relationship is not known by the individual who is being reported on. More information on the use of such sources is set out in Part 3.

2.8 Social Media can be a useful tool when investigating alleged offences but its use can, in some circumstances, amount to covert direct surveillance. More information on the use of Social Media in investigations is set out in Part 4.

## 3 SURVEILLANCE OF RESIDENTIAL PREMISES AND PRIVATE VEHICLES

3.1 There is a form of surveillance known as "intrusive surveillance" which is

3.1.1 carried out in relation to anything taking place on any residential premises or in any private vehicles; and

3.1.2 involves the presence of an individual on the premises or in the vehicle or is carried out by means of a surveillance device.

3.2 A surveillance device is one 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.

3.3 The Council cannot authorise Intrusive Surveillance.

## 4 WHEN WILL DIRECTED SURVEILLANCE BE AUTHORISED?

4.1 The Councils may only grant an authorisation for Directed Surveillance if it is necessary for the purpose of preventing or detecting conduct which:

a) constitutes:

i) one or more criminal offence; or
ii) is, or corresponds to, any conduct which, if it all took place in England and Wales would constitute one or more criminal offences; and

b) is an offence which:

i) is punishable on summary conviction, or indictment, by a maximum term of at least 6 months imprisonment; or
ii) is an offence under S.146 of the Licensing Act 2003; or
iii) is an offence under S.147 of the Licensing Act 2003; or
iv) is an offence under S.147A of the Licensing Act 2003; or
v) is an offence under S.7 of the Children and Young Peoples Act 1933.

For example, Directed Surveillance is not an option for the Councils when investigating minor offences such as dog fouling and littering, nor for tackling anti-social behaviour (unless the behaviour constitutes a criminal offence carrying a maximum sentence of 6 months or more), but may still be authorised for investigations into underage sales of alcohol and tobacco.

This provision does not apply to the Councils use of a Covert Human Intelligence Source (see part 3).

4.2 There is a formal application process for authorisation referred to in Part 2 of this document.

4.3 The person granting the authorisation must consider whether its effect would be proportionate to what is sought to be achieved by the surveillance. This involves balancing the intrusive effect on the person under investigation and others who might be affected (referred to as collateral intrusion) against the need for the surveillance. The surveillance will not be authorised if it is excessive in the circumstances of the case or if the information could be obtained by less intrusive means.

4.4 In considering the grant of the authorisation and in carrying out any subsequent surveillance the risk of intrusion upon the privacy of

persons not being investigated must be taken into account. Measures must be taken wherever possible to avoid or minimise such intrusion.

4.5 It is the responsibility of the Council Officer applying for the authorisation to justify the use of it and set this out fully on the relevant documentation referred to in Part 2.

4.6 Any authorisation granted by the Council must be submitted to a Justice of the Peace for consideration. The Justice of the Peace may either confirm or quash the authorisation. The authorisation cannot take effect until such time as an Order has been obtained approving the grant.

4.7 During the course of an investigation the type and seriousness of offences may change. If during the investigation it becomes clear that the activity being investigated does not amount to a criminal offence or that it would be a less serious offence that does not meet the threshold, the use of Directed Surveillance should stop and if a Directed Surveillance authorisation is already in force, it should be cancelled.

## 5 CONFIDENTIAL INFORMATION

5.1 Some information is likely to be particularly confidential or sensitive, including:

5.1.1 communications with a legal adviser;

5.1.2 information relating to the physical or mental health of an individual;

5.1.3 information relating to the spiritual counselling of an individual by a Minister of Religion;

5.1.4 confidential journalistic material.

Where such information is likely to be obtained, the authorisation should only be granted in exceptional and compelling circumstances (see paragraph 10.1).

## 6 VULNERABLE AND JUVENILE SOURCES

6.1 An authorisation for a Covert Human Intelligence Source (CHIS) who is in need of community care services by reason of mental or other disability, age or illness should only be granted in exceptional circumstances.

6.2 An authorisation for a Covert Human Intelligence Source (CHIS) who is under 18 years should only be granted after taking advice from the Solicitor to the Council and Monitoring Officer as to the effect of the

Regulation of Investigatory Powers (Juveniles) Order 2000 including the necessity for relevant risk assessments.

6.3 The use must not be authorised for a person under 16 years to provide information against his/her parents or any person who has parental responsibility for him/her.

## *7* LAWFULNESS

7.1 Surveillance will be lawful for all purposes if:

a) an authorisation, which has been confirmed by a Justice of the Peace, confers an entitlement to engage in the surveillance on the person(s) who carried it out; and

b) the surveillance is in accordance with the authorisation.

## 8 COMPLAINTS

8.1 The Investigatory Powers Tribunal ("IPT") is an independent body made up of senior members of the judiciary and the legal profession. It is independent of the Government.

8.2 An individual who is affected by surveillance undertaken by the Council may complain to the Tribunal at:

The Investigatory Powers Tribunal
PO Box 33220
London
SW1H 9ZQ

Tel: 0207 273 4514

8.3 More information about the IPT can be found at http://www.ipt-uk.com

8.4 The Councils also have an internal process for dealing with complaints. Any complaint recorded relating to surveillance should be referred to the Solicitor to the Council and Monitoring Officer at:

Adur and Worthing Councils
Town Hall
Chapel Road
Worthing
West Sussex
BN11 1HA

# PART 2 : PROCEDURE

## 9 APPLICATIONS

9.1 Authorisations may be applied for by any Officer of the Council who is carrying out, or is planning to carry out, an investigation in relation to suspected crime or disorder.

9.2 Authorisations are applied for on the forms set out in the Appendix, and have to be authorised, in writing, by an Authorising Officer.

9.3 Authorising Officers should usually avoid authorising their own activities. If this is unavoidable, then the authorisation record should be transparent by highlighting this.

9.4 Authorising Officers are to complete the authorisation or rejection in handwriting, and not typed script, so that if it is challenged they can identify their own writing and it can be clear that there has not been a “cut and paste” decision.

9.5 Following the granting of an authorisation by the Authorising Officer the authorisation must be submitted to a Justice of the Peace for consideration.

9.6 The Justice of the Peace may either confirm or quash the authorisation.

## 10 WHO ARE THE AUTHORISING OFFICERS AT THE COUNCILS?

10.1 When knowledge of confidential information is likely to be acquired (paragraph 5 above) or when a vulnerable individual or juvenile is to be used as a CHIS (paragraph 6) then only the Chief Executive or in his absence, his nominated Deputy, who shall be a Director, who has undertaken the appropriate training and is not the Senior Responsible Officer, can consider and grant the application, subject to judicial approval.

10.2 In all other cases, applications may be considered and granted, subject to Judicial approval, by:

a) the Chief Executive; or
b) a Director, who has undertaken the appropriate training on RIPA, other than the Senior Responsible Officer.

## 11 DURATION OF AUTHORISATIONS

### 11.1 Directed Surveillance

A written authorisation will cease to have effect (unless renewed) at the end of a period of three calendar months beginning with the day on which it took effect. An authorisation is to be cancelled at that time, but it can be renewed for a further three months, subject to Judicial approval. (See paragraph 14 below).

### 11.2 Covert Human Intelligence Source

A written authorisation will cease to have effect (unless renewed) at the end of a period of twelve calendar months beginning with the day on which it took effect. An authorisation is to be cancelled at that time. Subject to Judicial approval, an authorisation can be renewed for twelve months. (See paragraph 14 below).

An authorisation in respect of a juvenile is limited to one month's duration.

## 12 APPLICATION FOR JUDICIAL APPROVAL

12.1 Once the application, whether for Directed Surveillance or for the use of a CHIS, has been authorised by the Councils' Authorising Officer the Authorising Officer shall contact the Sussex Magistrates Administration Centre on:

ss-sussexadmin@hmcts.gsi.gov.uk

01273-670888

The best Officer to make the application for judicial approval is the Authorising Officer as only he/she can answer questions about his reasoning on necessity, proportionality, collateral intrusion and risk.

12.2 A straightforward application will be listed before a presiding Magistrate.

12.3 Complicated applications are to be listed before District Judge Crabtree when sitting at Worthing Magistrates' Court.

12.4 The authorisation, whether for Directed Surveillance or for the use of a CHIS, cannot take effect until an Order has been obtained from a Justice of the Peace approving the renewal or grant of an authorisation. If the Justice of the Peace is satisfied that the statutory tests have been met and that the use of the technique is necessary and proportionate, they will issue an order approving the grant or renewal for the use of the technique as described in the application.

## 13 REVIEWS

### 13.1 Directed Surveillance

The Authorising Officer must, in relation to each authorisation determine how often the authorisation is to be reviewed, taking into account the nature and purpose of the surveillance authorised. Regular reviews of authorisations should be undertaken to assess the need for the surveillance to continue. The results of a review should be recorded on the central record of authorisations. Particular attention is drawn to the need to review authorisations frequently when the surveillance provides access to confidential information or involves collateral intrusion.

The forms in the Appendix are to be used.

### 13.2 Covert Human Intelligence Source

Regular reviews of authorisations should be taken to assess the need for the use of a source to continue. The review should include the use made of the source during the period authorised, the tasks given to the source and the information obtained from the source. The results of the review should be recorded on the authorisation record. Particular attention is drawn to the need to review authorisations frequently where the use of a source provides access to confidential information or involves collateral intrusion.

The forms in the Appendix are to be used.

## 14 RENEWALS

### 14.1 Directed Surveillance

14.1.1 If, at any time before an authorisation would cease to have affect the Authorising Officer considers it necessary for the authorisation to continue for the purposes for which it was given, he/she may renew it, in writing, for a further period of three months, subject to further Judicial approval.

14.1.2 Applications for renewal shall be in writing on the form set out in the Appendix.

14.1.3 Following the granting of a renewed authorisation by the Authorising Officer the authorisation must be submitted to a Justice of the Peace for consideration.

14.1.4 The Justice of the Peace may either confirm or quash the authorisation.

14.1.5 Authorisations may be renewed more than once, if necessary, and the renewal should be kept/recorded as part of the central record of authorisations.

14.2 **Covert Human Intelligence Source**

14.2.1 If, at any time before an authorisation would cease to have effect the Authorising Officer considers it necessary for the authorisation to continue for the purposes for which it was given, he may renew it, in writing, for a further period of twelve months, subject to further Judicial approval.

14.2.2 Applications for renewal shall be in writing on the form set out in the Appendix.

14.2.3 Before an Authorising Officer renews an authorisation he/she must be satisfied that a review has been carried out of the use of the source.

14.2.4 Following the granting of an authorisation by the Authorising Officer the authorisation must be submitted to a Justice of the Peace for consideration.

14.2.5 The Justice of the Peace may either confirm or quash the application.

14.2.6 Authorisations may be renewed more than once, if necessary, and the renewal should be kept/recorded as part of the central record of authorisation.

## 15 CANCELLATION

15.1 The Authorising Officer who granted, or last renewed, the authorisation must cancel it if he/she is satisfied:-

15.1.1 that the Directed Surveillance or use of the source no longer meets the criteria upon which it was authorised, or

15.1.2 that satisfactory arrangements for the source used no longer exist.

Where the Authorising Officer is no long available, this duty will fall to the person who has taken over the role of Authorising Officer, or the person who is acting as Authorising Officer.

The forms in the Appendix are to be used.

15.2 As soon as the decision is taken that Directed Surveillance or use of a source should be discontinued, the instruction must be given to those involved to stop all surveillance of the subject(s). The date and time when such an instruction was given should be recorded in the central record of authorisations and the notification of cancellation where relevant.

The forms in the Appendix are to be used.

## 16 HANDLING, STORAGE, USE AND DESTRUCTION OF MATERIAL AS EVIDENCE

16.1 All materials or records of information obtained as a result of Directed Surveillance, or the use of a source, must be stored for no longer than is necessary. Authorising Officers must ensure compliance with appropriate Data Protection requirements and any relevant guidance produced by the Councils relating to the handling and storage of material.

16.2 The product of surveillance described in this Policy must be retained until a decision is made whether or not to take proceedings. If proceedings are instituted, material must be retained until the matter is disposed of. If the subject of the surveillance is prosecuted in criminal proceedings and is convicted the material must be retained until:

16.2.1 the completion of any appeal process;

16.2.2 if sentenced to custody or a hospital Order, until his/her release, if more than 6 months after conviction;

16.2.3 in other cases, 6 months after any Order made is discharged or expires by effluxion of time.

16.3 There is a duty to disclose in criminal proceedings information which has been gathered as part of the investigation and may be relevant to it.

16.4 If civil proceedings are taken, then material is to be kept until 6 months after any Order made is discharged or expires by effluxion of time.

## 17 CENTRAL RECORD OF ALL AUTHORISATIONS

17.1 The Solicitor to the Council and Monitoring Officer, the RIPA Co-ordinator, shall maintain a central register of all authorisations, which is regularly updated whenever an authorisation is granted, renewed or cancelled. The entry in the register shall be retained for a period of three years from the ending of the authorisation.

17.2 The central register shall contain the information listed in the Appendix.

17.3 Within 24 hours of taking any action in relation to an authorisation that is to be recorded in the register the Authorising Officer shall provide sufficient details of that action, in writing, to the Solicitor to the Council and Monitoring Officer.

## 18 RECORD KEEPING

### 18.1 Directed Surveillance

The Authorising Officer shall maintain the following documentation, which shall be cross-referenced with the central register by use of a unique reference number:-

18.1.1 a copy of the application and a copy of the authorisation, together with any supplementary documentation and notification of the approval given by the Authorising Officer;

18.1.2 a record of the period over which the surveillance has taken place;

18.1.3 the frequency of reviews prescribed by the Authorising Officer;

18.1.4 a record of the result of each review of the authorisation;

18.1.5 a copy of any renewal of an authorisation, together with the supporting documentation submitted when the renewal was requested.

18.1.6 the date and time when any instruction was given by the Authorising Officer.

### 18.2 Covert Human Intelligence Sources

The Authorising Officer shall maintain the following documentation, which shall be cross-referenced with the central register by use of a unique reference number:-

18.2.1 a copy of the application and the authorisation, together with any supplementary documentation and notification of the approval given by the Authorising Officer;

18.2.2 a copy of any renewal of an authorisation, together with the supporting documentation submitted when the renewal was requested;

18.2.3 the reason why the person renewing the authorisation considered it necessary to do so;

18.2.4 any authorisation which was granted or renewed orally (in an urgent case) and the reason why the case was considered urgent;

18.2.5 any risk assessment made in relation to the source;

18.2.6 the circumstances in which tasks were given to the source;

18.2.7 the value of the source to the investigating authority;

18.2.8 a record of the results of any reviews of the authorisation;

18.2.9 the reasons, if any, for not renewing the authorisation;

18.2.10 the reason for cancelling an authorisation;

18.2.11 the date and time when any instructions were given by the Authorising Officer to cease using a source.

The records kept should:

a. Hold the name of the source and the information in different places.

b. The information file should only identify the source by way of a unique reference number.

c. The file identifying the source must be retained in secure storage and be held by the relevant Authorising Officer.

d. With each source the relevant Authorising Officer shall direct which Head of Service shall have responsibility for maintaining a record of the use made of the source.

## PART 3 : USE OF COVERT HUMAN INTELLIGENCE SOURCES

### 19 DEFINITION

19.1 A person is a Covert Human Intelligence Source if:-

19.1.1 he/she establishes or maintains a personal or other relationship with a person for the covert purposes of

facilitating the doing of anything falling within paragraphs 19.1.2 or 19.1.3 below.

19.1.2 he/she covertly uses such a relationship to obtain information or to provide access to any information relating to any person, or

19.1.3 he/she covertly discloses information obtained by the use of such a relationship or as a consequence of the existence of such a relationship.

19.2 A relationship or disclosure is covert if it is conducted in a manner which is calculated to ensure that one party to it is unaware of its use and purpose.

19.3 For a person to come into the category of a CHIS there is no requirement for the Councils to actively engage the person in that role. The question to be asked is whether a person is using a relationship to covertly obtain information which he/she is passing to the Councils.

For example, if Mr. Y volunteers information to the Councils about a work colleague then he is not a CHIS. However, if the Councils go back to Mr. Y and ask him to ascertain information about the work colleague and Mr. Y attempts to ascertain that information then he is a CHIS and an authorisation should be obtained.

Further, if Mr. Y. volunteers information to the Councils about a work colleague, then on the initial passing of information he is not a CHIS. However, if he then continues to gather information covertly and passes it to the Councils, there is a point at which he will become a CHIS and therefore Officers should be aware that if a person is providing information about another person on more than one occasion it is necessary to consider whether or not the person providing the information is exploiting their relationship with the third party to covertly obtain information. If so, then a CHIS authorisation is to be obtained.

## 20 TASKING AND SUPERVISION

20.1 A Council Officer must be designated to have day-to-day responsibility for:

20.1.1 dealing with the source;

20.1.2 directing his/her day-to-day activities;

20.1.3 recording the information supplied by the source;

20.1.4 monitoring his/her security and welfare.

20.2 A separate Officer, at Head of Service level, must also be given responsibility for the general oversight of the use of the source.

## 21 SECURITY AND WELFARE

21.1 The Councils must take into account the safety and welfare of the source when carrying out actions in relation to an authorisation or tasking. It should also have regard to any foreseeable consequences to others of the tasking of the source.

21.2 Prior to authorisation, a risk assessment must be carried out to determine the risks to the source of any tasking and the likely consequences should the role of the source become known. The ongoing security and welfare of the source after the end of the authorisation should also be considered at the outset. Records disclosing the identity of the source will not be available to persons unless there is a proven need to disclose them for operational reasons.

21.3 If the Officer having day-to-day responsibility for the source (paragraph 20.1) has any concerns about the personal circumstances of the source in so far as they might effect

- The validity of the risk assessment;
- The conduct of the source;
- The safety and welfare of the source;

he/she shall draw these to the attention of the Supervising Officer (paragraph 20.2). A decision must be made whether to (1) refer these concerns to the Authorising Officer and (2) seek a review of the authorisation.

## 22 TELEPHONE INTERCEPTION

Where one party to a telephone communication consents to its interception by a third party, it is treated as Directed Surveillance and may be authorised as such.

## 23 USE OF TECHNICAL EQUIPMENT

23.1 A source may be present on residential premises or in a private vehicle. If he/she is using a surveillance device, no authorisation for intrusive surveillance would be required to record any activity taking place on those premises or in the vehicle if it is in his/her presence. In

other circumstances an authorisation for intrusive surveillance would be required and this is outside the powers of the Council.

# PART 4: USE OF SOCIAL MEDIA IN INVESTIGATIONS

## 24 BACKGROUND

24.1 Social Media accumulates a sizable amount of information about a person's life and can provide incredibly detailed information about a person and their activities. Social Media can therefore be a very useful tool when investigating alleged offences.

24.2 Whilst the use of Social Media to investigate is not automatically considered covert surveillance, its misuse when conducting investigations can mean that it crosses over into the realms of covert surveillance even when that misuse is inadvertent. It is therefore crucial that the provisions of RIPA, as it relates to covert and directed surveillance, are followed at all times when using Social Media information in investigations.

24.3 It is possible for the Councils' use of Social Media in investigating potential offences to cross over into becoming unauthorised surveillance, and in so doing, breach a person's right to privacy under Article 8 of the Human Rights Act. Even if surveillance without due authorisation in a particular instance is not illegal, if authorisation is not obtained, the surveillance carried out will not have the protection that RIPA affords and may mean it is rendered inadmissible.

24.4 Council Officers embarking on any form of investigatory action should always do so with RIPA in mind. Whilst RIPA will not always be relevant to every investigation, it is vital that Officers involved in investigative practices against individuals, regularly review their conduct with respect to investigatory actions. Any investigation is capable of evolving from being one that does not require RIPA authorisation, to one that does, at any point.

## 25 WHAT IS MEANT BY SOCIAL MEDIA?

25.1 Social Media can take many forms but will always be a web-based service that allows individuals and/or businesses to construct a public or semi-public profile. It will often have some, or all, of the following characteristics:

- The ability to show a list of other users with whom they share a connection, often termed ‘friends’ or ‘followers’;
- The ability to view and browse their list of connections and those made by others within the system;
- Hosting capabilities allowing users to post audio, photographs and/or wide content that is viewable by others.

The number and type of social media available to the public is fluid but currently includes Facebook, Twitter, Instagram, LinkedIn, Pintrest, Tumblr, Reddit, Flickr and Google+.

## 26 WHEN WOULD THE USE OF SOCIAL MEDIA REQUIRE AUTHORISATION?

### 26.1 Privacy settings

26.1.1 The majority of Social Media services will allow its users to decide who can view their activity, and to what degree, through the use of privacy settings. Many users will purposely use Social Media with no privacy settlings applied whatsoever and this information publicly available is known as an individual’s public profile. Whilst the content or information shared by individuals on Social Media remains the property of that individual, it is nonetheless considered to be in the public domain.

### 26.2 Private Profile

26.2.1 By setting a profile to private, a user does not allow everyone to access and use their content, and respect should be shown to that person’s right to privacy under Article 8 of the Human Rights Act. If access controls are applied, the individual has a reasonable expectation of privacy. This does not, however, extend to instances where a third party takes it upon themselves to share information which originated on a private profile on their own social media profile.

26.2.2 However, if it is necessary and proportionate for the Councils to covertly breach access controls, the minimum requirement is an authorisation for Directed Surveillance.

26.2.3 An authorisation for the use and conduct of a CHIS is necessary if a relationship is established or maintained by a Council Officer or by a person acting on the Councils’ behalf, for example where there is interaction and two way communication rather than merely reading of the social media site’s content. Should a Council Officer set up a false identity for a covert purpose with a view to conducting Directed Surveillance to obtain private information, an authorisation would certainly be required. Should a Council Officer adopt the identity of a person known, or likely to be known, to the individual, authorisation would be required, along with the explicit written consent of the person whose identity is being used, and careful thought would need to be given as to how to protect that person.

### 26.3 Public Profile

26.3.1 Where a person publishes content on a public profile they allow everyone, including those not on that particular Social Media platform, to access and use that information whilst allowing it to be associated with them. In practice, this means that things such as photographs, video content or any other relevant information posted by individuals and businesses to a public profile on any given Social Media platform can be viewed, recorded and ultimately used as evidence against them should the matter end in legal proceedings, subject to the usual rules of evidence.

26.3.2 Where privacy settings are available but not applied the data may be considered open source and RIPA authorisation is not usually required. However a distinction is made between one-off and repeated visits to an individual's Social Media profile. Whilst one-off visits, or otherwise infrequent visits spread over time, cannot be considered to be Directed Surveillance, repeated or frequent visits may cross over into becoming Directed Surveillance requiring RIPA authorisation. A person's Social Media profile should not, therefore, be routinely monitored on a daily or weekly basis in search of updates, as that would, in all likelihood constitute Directed Surveillance and require authorisation.

## 27 COLLATERAL DAMAGE

27.1 Due to the nature of Social Media, there is a significant risk of collateral damage in the form of other, innocent parties' information being inadvertently captured alongside that of the suspected offender's. When capturing evidence from a social media profile, steps should be taken to minimise this collateral damage either before capturing the evidence, or subsequently through redaction. This might be particularly prevalent on social media profiles promoting certain events, where users are encouraged to interact with each other by posting messages or on photographs where other users may be making comments.

## 28 RETENTION AND DESTRUCTION OF INFORMATION

28.1 Due to the nature of Social Media, it is important to remember that when information produced as a hard copy is destroyed in line with this Policy, that all digital copies of that evidence is likewise destroyed.

# PART 5 : REFERENCES

a) Regulation of Investigatory Powers Act 2000 (Chapter 2, Part 2).

b) Home Office codes of practice on Directed Surveillance and Covert Human Intelligence Sources.

c) Regulation of Investigatory Powers (Directed Surveillance and Covert Human Intelligence Sources) Order 2003 SI 2003/3171.

d) Regulation of Investigatory Powers (Juveniles) Order 2000 – SI 2000/2793.

e) Regulation of Investigatory Powers (Extension of Authorisation Provisions: Legal Consultations) Order 2010

f) The Office of the Surveillance Commissioner at www.surveillancecommissioners.gov.uk

g) Protection of Freedoms Act 2012

h) Regulation of Investigatory Powers (Directed Surveillance and Covert Human Intelligence Sources) Order 2010, SI 2010/521

i) The Regulation of Investigatory Powers (Directed Surveillance and Covert Human Intelligence Sources) (Amendment) Order 2012, SI 2012/1500

## Appendix

| **Forms** | **Located** |
|---|---|
| **Directed Surveillance** | |
| Application for authorisation | Councils' intranet |
| Review | Councils' intranet |
| Renewal | Councils' intranet |
| Cancellation | Councils' intranet |
| **Covert Human Intelligence Source** | |
| Application for authorisation | Councils' intranet |
| Review | Councils' intranet |
| Renewal | Councils' intranet |
| Cancellation | Councils' intranet |
| **Judicial Application** | |
| Application for judicial approval | Councils' intranet |
| Draft Judicial Order | Councils' intranet |
| **Register of Authorisations** | Held by Solicitor to the Council and Monitoring Officer |