SURVEILLANCE UNDER THE REGULATION OF INVESTIGATORY POWERS ACT 2000 (RIPA)

POLICY AND PROCEDURES

December 2015

1.0 INTRODUCTION

The Regulation of Investigatory Powers Act 2000 (RIPA) provides a regulatory framework to enable public authorities to obtain information through the use of certain covert investigatory techniques.

The Protection of Freedoms Act 2012, which came into force on 1st November 2012, requires that applications to use covert surveillance techniques must have prior judicial approval. In addition, restrictions limiting the use of surveillance to the investigation of offences which attract a custodial sentence of six months or more have been introduced for certain types of surveillance activity.

2.0 BACKGROUND

An individual has rights, freedoms and expectations, which are guaranteed by the European Convention and the Human Rights Act 1998. Respect for these rights is fundamental to the operation of government within the UK. Using RIPA powers can conflict with and cause the suspension of an individual's human rights, and so it is imperative that, when investigating wrongdoing, certain conditions are met in each case, in order that successful prosecutions can be made.

In particular, RIPA requires that covert techniques are only used when it is necessary and proportionate to do so. Compliance with RIPA will significantly reduce the likelihood of any surveillance carried out by the Council being unlawful, and therefore subject to legal challenge.

Surveillance by a public authority is likely to constitute an infringement of and suspension of an individual's rights and freedoms which are protected by the Human Rights Act 1998. However, by following the authorisation procedures set out by RIPA, officers of the Council are ensuring that they can demonstrate that the surveillance is necessary for a purpose permitted by the Human Rights Act 1998 and that it is a proportionate measure to take, given all the circumstances.

Cheshire East Council will, on occasion, need to use covert surveillance in order to carry out its enforcement functions effectively. Examples of enforcement activities which may require the use of RIPA include benefit fraud, planning enforcement, licensing enforcement, trading standards, environmental health and community safety investigations. RIPA powers can be used where it is demonstrated that viable alternatives to obtaining evidence to mount a prosecution have been considered, but are not appropriate. A local authority may only use covert surveillance for the purpose of the prevention or detection of serious crime.

3.0 USE OF COVERT SURVEILLANCE IN LOCAL AUTHORITIES

Local authorities are not authorised to carry out any form of intrusive surveillance. **Intrusive surveillance** is defined in Section 26 (3) of RIPA as:

- covert surveillance, which is carried out in relation to anything taking place on any residential premises or in any private vehicle; and involves the presence of an individual on the premises or in the vehicle, or is
- carried out by means of a surveillance device (e.g. a listening or tracking device in a person's home or in his/her private vehicle).

Local authorities are restricted to three techniques they are permitted to undertake within covert surveillance, i.e.

- using 'directed' surveillance
- deploying a Covert Human Intelligence Source (CHIS)
- acquiring communications data.

Before using any of these three techniques, the local authority is required to obtain the authorisation of a very senior officer of the Council and, additionally, ensure that approval has been granted by a Justice of the Peace/Magistrate.

3.1 Types of surveillance available to Local Authorities

'**Directed Surveillance'** is essentially covert surveillance in places open to the public. It is defined as

- Covert
- Likely to obtain private information
- Carried out in a publicly accessible place
- Pre-planned against a specific individual or group
- Conducted otherwise than as an immediate response to events

It includes surveillance by person or device to:

- Observe someone's movements
- Eavesdrop on conversations
- Photograph or film people or events
- Track vehicles

A further restriction has been placed on the use of directed surveillance to prevent local authorities using this for low-level cases. The Protection of Freedoms Act 2012 introduced a crime threshold, whereby local authorities will only be able to use this power when investigating offences which attract a custodial sentence of six months or more or an offence relating to the sale of alcohol or tobacco products to minors.

3.2 A 'Covert Human Intelligence Source' (CHIS) can be either an undercover officer or a member of the public acting as an informant. The CHIS is someone who

- establishes and maintains a relationship for a covert purpose
- covertly uses the relationship to obtain information or to provide access to information from another person
- covertly discloses the information derived from the relationship to the Council

Where the CHIS is under 18, special risk assessments need to be carried out for each case.

3.3 Access to communications Data

Under RIPA legislation, the Council is limited to accessing only service user and subscriber data, i.e. the 'who', 'when' and 'where' of a communication – not the actual content.

4.0 APPLYING THE RIPA PRINCIPLES

4.1 The tests of necessity and proportionality

Use of covert surveillance should only be authorised if the Authorising Officer is satisfied that the action is both **NECESSARY** (in a democratic society) for the prevention or detection of serious crime and **PROPORTIONATE**. The Human Rights Act defines a measure or action as proportionate if it:

- impairs as little as possible the rights and freedoms (of the individual concerned and of innocent third parties), and
- is carefully designed to meet the objectives in question, is not arbitrary, unfair or based on irrational considerations.

4.2 Collateral intrusion

In the case of both directed covert surveillance and the use of a covert human intelligence source, the Authorising Officer must also take into account the risk of intrusion into the privacy of persons other than those who are directly the subject of the investigation or operation. This is termed "collateral intrusion". Officers 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. Consideration should be given to whether the authorisation should be amended and re-authorised or whether a new authorisation is required.

5.0 PROCEDURES FOR IMPLEMENTING COVERT SURVEILLANCE

5.1 General

All covert surveillance must be properly authorised and recorded, the tests of necessity and proportionality must be satisfied, and the potential for collateral intrusion must be considered and minimised. Authorisations must be granted by a Magistrate before any activity takes place.

Any officer intending to undertake covert surveillance or use a covert human intelligence source must only do so if other means of obtaining it have been considered but are not viable.

Embarking upon covert surveillance or the use of a covert human intelligence source without authorisation, or conducting covert surveillance outside the scope of the authorisation, will not only mean that the "protective umbrella" of RIPA is unavailable, but may result in disciplinary action being taken against the officer/officers involved. It may result in the criminal investigation being compromised as the evidence will be considered to have been obtained unlawfully.

All relevant Council contracts issued to contractors/subcontractors must include a term that this policy and associated procedures are to be observed when operating on behalf of the Council.

Directed surveillance may only be carried out on residential premises if a member of the public has requested help or made a complaint to the Council, and if written permission to conduct the surveillance has been obtained from the householder or tenant from whose premises the surveillance will be carried out.

5.2 Closed Circuit Television (CCTV)

CCTV systems are not normally within the scope of RIPA. However, if they are used for a specific operation or investigation, or if automatic facial recognition by means of CCTV is used, authorisation for the use of directed surveillance must be obtained by the investigating officer either from the Police or the Council depending on who is leading the investigation.

5.3 Social Networking Sites (SNS) and other Internet sites

The fact that digital investigation is easy to conduct does not reduce the need for authorisation when necessary and consideration must be given to whether authorisation under RIPA should be obtained.

Care must be taken to understand how the SNS being used works and 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.

It is the responsibility of individuals to set privacy settings to protect against unsolicited access to their private information. Unprotected data may be deemed published and no longer under the control of the author but there is a reasonable

expectation of privacy if access controls are applied. Where privacy settings are available and not applied the data may be considered 'open source' and an authorisation is not usually required. However, repeat viewing of "open source" sites may be deemed directed surveillance and this should be borne in mind.

If it is necessary and proportionate for the Council to covertly breach access controls, an authorisation for directed surveillance will be required. Consideration may need to be given to authorisation of a CHIS if the Council wishes to establish a relationship with an individual through a SNS or website, i.e. if the activity is more than mere reading of the site's content.

An officer of the Council must not set up a false identity for covert purposes without authorisation.

5.4 Officers able to make authorisations

.
Under the Regulation of Investigatory Powers (Directed Surveillance and Covert Human Intelligence Sources Order 2010 (2010/521), the role of Authorising Officer for local authorities is restricted to the Chief Executive and Executive Directors. For applications for directed surveillance and the acquisition of communications data, the Authorising Officers for the Council are, similarly, the Chief Executive and members of the Management Group Board. The Director of Legal Services is not an Authorising Officer, as this post assumes responsibility as the Monitoring Officer, to ensure that the Council complies with the requirements of RIPA legislation.

In cases which require the use of a CHIS, or cover confidential information, e.g. it is subject to legal privilege or confidential personal information, which is particularly sensitive, the Authorising Officer is the Chief Executive or, in his or her absence, an Executive Director or the Chief Operating Officer. Authorising Officers should not be responsible for authorising investigations or operations in which they have had or are likely to have any direct involvement. When such authorisation is required, this should be sought from an alternative Authorising Officer, as appropriate.

5.5 Authorisation for access to communications data

The legislation requires that a Home Office accredited person, a Single Point of Contact (SPOC), facilitates the acquisition of the communications data requested. The SPOC can be either an officer of the council or a member of an external organisation. Local authorities are permitted to use the services of the National Anti Fraud Network (NAFN) to scrutinise applications and provide advice, to ensure the Authority acts in an informed and lawful manner. By doing this, the Authority avoids the requirement of appointing an individual officer who has received Home Office accreditation. The accredited officers at NAFN scrutinise applications independently and, following final approval from the Justice of the Peace/Magistrate, acquire the communications data on behalf of the Council. The use of NAFN is to be reviewed on an annual basis.

5.6 The role of the Investigating Officer

It is the responsibility of the Investigating Officer to present the facts of the application, i.e.

- the crime to be investigated and the offence/sentence it attracts
- the reasons why it is proposed to conduct the investigation covertly
- what covert tactics are requested and why
- on whom the covert surveillance will be focused and who else may be affected by it
- how it is intended to conduct the surveillance
- the Who, What, When, Why & How

5.7 The role of the Authorising Officer

It is the role of the Authorising Officer to:

- demonstrate his/her satisfaction that use of covert surveillance is necessary for the crime being investigated by setting out in their own words why they are satisfied the activity is necessary
- demonstrate how he/she has reached the conclusion that the activity is proportionate to what it seeks to achieve and the reasons why the methods are not disproportionate
- ensure the application states explicitly what is being authorised, against which subjects, property or location. It is his/her responsibility to ensure those who conduct the surveillance are clear on what has been authorised.

In order to give proper consideration to the potential for collateral intrusion, the Authorising Officer must fully understand the capabilities and sensitivity levels of equipment intended to be used and where and how it is to be deployed. He/she may require a Privacy Impact Assessment to be prepared. Particular care should be taken when data or information is obtained from open or unevaluated sources such as the internet or social networking sites. (See paragraph 5.3)

5.8 The role of the Justice of the Peace/Magistrate

Under the Protection of Freedoms Act 2012, authorisations/applications will not come into effect unless and until approval by a Justice of the Peace has been obtained. Applications to a Justice of the Peace for an order, approving the granting or renewal of a RIPA application, will include the signed detailed authorisation form, along with a Judicial Application for Approval form, to be completed by the local authority, and an order which the Justice of the Peace will complete in order to record his/her decision.

The role of the Justice of the Peace is to examine the RIPA form, consider the justification for use of the technique, and cross-examine an attending Local Authority representative, if it is necessary to clarify particular points, and finally, record his/her decision.

The form and supporting papers must by themselves make the case. It is not sufficient for the Justice of the Peace to rely on oral evidence, where this is not

reflected or supported. The Council's Investigating Officer will be required to attend as the local authority representative to answer any queries the JP may have.

5.9 Outcomes

The order which the Justice of the Peace will complete, reflecting his/her decision, will identify one of the three following potential outcomes:

- Approval granted.
- Approval refused - the Council may not use the covert technique but may re-apply if significant new information comes to light or if technical errors in the initial application have been addressed.
- Refuse and Quash – the council may not use the covert technique. This decision might be used where the JP is of the opinion the application is fundamentally flawed.

5.10 The role of the Director of Legal Services/Monitoring Officer

The Director of Legal Services/Monitoring Officer is designated as being responsible for the integrity of the process as follows:

- ensuring compliance with all relevant legislation and with the Codes of Practice
- engagement with the Inspectors from the Office of the Surveillance Commissioner when they conduct their inspections and, where necessary, oversight of the implementation of post-inspection action plans approved by the relevant oversight Commissioner
- monitoring authorisations and conducting a quarterly review of applications, authorisations, refusals, reviews, renewals and cancellations.

5.11 The role of Elected Members

It is considered good practice for Elected Members to undertake a formal scrutiny role in relation to RIPA, and review the Council's use of it on an annual basis. However, they should not be involved in making decisions on specific authorisations.

The Monitoring Officer should ensure that an Annual Report regarding the Council's use of RIPA is submitted to the Council's Audit & Governance Committee. The report should include details of the overall number and type of authorisations granted and the outcome of the case, where known. In addition, the report should provide a breakdown of the same information by service or groups of services, as appropriate.

The report should also include the results of the most recent inspection conducted by a representative of the Office of Surveillance Commissioners, where applicable.

6.0 PROCEDURES FOR GAINING APPROVAL

6.1 General

At departmental level, the application for authorisation must be in writing (electronically typed) and on the appropriate form, which must be completed in full. Officers should ensure that they use the current form available directly from the Home Office website (https://www.gov.uk/government/collections/ripa-forms--2).

Before applications are authorised they must be forwarded to the Compliance and Customer Relations Team to be checked by an approved 'Review Panel', currently made up of Compliance & Customer Relations Manager, Senior Compliance & Customer Relations Officer and Community Safety Delivery Manager (RIPA Trainer), and recorded in the **Central Record of Authorisations**. A unique reference number will be allocated at this stage. Officers requesting authorisation for directed surveillance should complete a risk assessment, which should be submitted with the authorisation request.

Officers requesting authorisation to use a covert human intelligence source ("CHIS") must always complete a risk assessment and submit it with the authorisation request

6.2 Document retention

All relevant documentation, including a copy of the authorisation, a record of the period over which surveillance has taken place, any risk assessment, notebooks, surveillance logs and other ancillary documentation should be retained at departmental level for a period of six years from the date of commencement of the surveillance, at which point they should be securely destroyed.

6.3 Duration of authorisations

Authorisation of directed surveillance will cease to have effect (unless renewed) either on specific cancellation (within the period of three months) or at the end of a period of three months (directed surveillance) or twelve months ("CHIS"), beginning with the day on which the authorisation was granted by the Justice of Peace/Magistrate.

6.4 Reviews

Regular monthly reviews of authorisations should be undertaken by the Authorising Officer to assess the need for surveillance to continue. The Council has chosen to instigate more frequent fortnightly reviews. All reviews should be completed using the appropriate form. It is important to note that reviews cannot broaden the scope of the original authorisation, but can reduce it for minor changes.

6.5 Renewals

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 purpose for which it was given, he/she may renew it in writing. All applications for the Renewal of an Authorisation for Directed Surveillance should be on the appropriate form, which must be completed in full.

6.6 Cancellations and handling of surveillance material

It is a statutory requirement that authorisations are cancelled as soon as they are no longer required. The Authorising Officer (or Investigating Officer in the first place) who granted (or last renewed) the authorisation must cancel it, if he is satisfied that the activity no longer meets the criteria for which it was authorised, or that it has fulfilled its objective.

If the Authorising Officer is no longer available, this duty will fall to the person who has taken over the role of the Authorising Officer. On cancellation of an authorisation, the Authorising Officer must be satisfied that the product of any surveillance is properly retained and stored or destroyed. If the surveillance product is of no evidential or intelligence value, it should be destroyed without delay, in accordance with Data Protection requirements. If the surveillance product is of potential evidential or intelligence value, it should be retained on the legal file, in accordance with established disclosure requirements, commensurate with any subsequent review.

When cancelling an authorisation, the Authorising Officer should:

- record date and times that surveillance took place and date the order to cease activity was made
- record reason for cancellation
- ensure surveillance equipment is removed and returned
- provide direction for management of product
- record value of surveillance, i.e. whether objectives of activity were met

6.7 Cessation of activity

As soon as the decision is taken that the authorised activity should be discontinued, the instruction must be given to those involved to stop all surveillance of the subject, or to cease using the covert human intelligence source. Documentation detailing the date and time when any cancellation instruction was given by the Authorising Officer should be retained for a period of six years, at which point it should be securely destroyed.

6.8 Central Record of Authorisations

The Compliance and Customer Relations Team is responsible for ensuring that a Central Record of Authorisations is maintained. This must be updated whenever an authorisation is granted, reviewed, renewed or cancelled. The record should be made available to the relevant Commissioner or an Inspector from the Office of Surveillance Commissioners, upon request. These records should be securely retained for a period of three years from the ending of the authorisation, at which point they must be securely destroyed. It is necessary that the original hand signed (wet signature) authorisation is maintained within the Central Record of Authorisations, to provide a valid audit trail for court purposes. The Compliance and Customer Relations Team also retain copies of other RIPA forms such as those from the DWP where CEBC staff are involved in surveillance but are not the lead officers. The Monitoring Officer should review and sign this Record on a quarterly basis.

With regard to **'directed' surveillance** the Central Record of Authorisations will contain a copy of the authorisation, together with the following information:

- the type of authorisation
- the date the authorisation was given
- the name of the Authorising Officer
- the departmental reference number of the investigation or operation
- the title of the investigation or operation, including a brief description and names of subjects, if known
- date of approval from Magistrates Court, name of Magistrate and outcome
- whether the urgency or oral provisions were used, and if so why
- in the case of a self authorisation by the Authorising Officer, a statement in writing that he/she expressly authorised the action (only in exceptional circumstances)
- if the authorisation is renewed, the date of renewal and who authorised it, including the name and grade of the Authorising Officer
- whether the investigation or operation is likely to result in obtaining confidential information
- the date of cancellation of the authorisation
- where collateral intrusion may be an issue, a copy of the Privacy Impact Assessment

With regard to a **covert human intelligence source ("CHIS"),** the Central Record of Authorisations must contain the following additional information:

- a copy of the authorisation, together with any supplementary documentation and notification of the approval given by the Authorising Officer
- a copy of any renewal of an authorisation, together with the supporting documentation submitted when the renewal was requested
- the reason why the person renewing an authorisation considered it necessary to do so
- any urgent authorisation which was granted or renewed orally (in an urgent case) and the reason why the case was considered urgent
- the risk assessment made in relation to the source ("CHIS")
- a record of the results of any reviews of the authorisation
- the reasons, if any, for not renewing an authorisation
- the reasons for cancelling an authorisation - cancellations are to be completed on the appropriate form
- the date and time when any instruction was given by the Authorising Officer to cease using a "CHIS"
- where collateral intrusion may be an issue, a copy of the Privacy Impact Assessment

With regard to **Applications for Communications Data,** a separate Central Record of Authorisations will be maintained which will contain:

- a copy of the authorisation together with the following information:
- applicant's name and job title
- the operation name, including a brief description of the nature of the operation and names of subject(s) if known

- the name and job title of Designated Officer
- name of the accredited SPOC
- date the authorisation was given by the Designated Officer
- date of approval from the Magistrate's Court, name of Magistrate and outcome

6.9 Additional requirements for authorisation of covert human intelligence sources only

6.9.1 Covert human intelligence sources may only be authorised if the following additional arrangements are in place:

- There is an employee of the Council with day to day responsibility for dealing with the source and, for the source's security and welfare, there is a Senior Officer who has general oversight of the use made of the source.
- An officer who is responsible for maintaining a record of the use made of the source; these records will contain any matters specified by the Secretary of State – The Regulation of Investigatory Powers (Source Records) Regulations 2000 (SI 2000/2725) set out these matters.
- Records disclosing the identity of the source and the information provided by him/her will not be made available to others except on a need to know basis

6.9.2 Vulnerable individuals (i.e. a person who is in need of community care services by reason of mental or other disability, age or illness and who is or may be unable to take care or protect himself against significant harm or exploitation) may be authorised to act as a CHIS only in the most exceptional circumstances.

6.9.3 Authorisations for juvenile sources (under 18) should only be granted if the provisions contained in The Regulation of Investigatory Powers (Juveniles) Order 2000 (SI 2000/2793) are satisfied. Any authorisation should be granted by the Chief Executive or (in his/her absence) an Executive Director or the Chief Operating Officer. The duration of an authorisation for the use or conduct of juvenile sources is one month.

6.9.4 If a juvenile source (under 18) is to be used, the Authorising Officer is responsible for obtaining the written consent of the parent or guardian or the person caring for the juvenile, unless to do so would compromise the juvenile's welfare or safety. The Authorising Officer is also responsible for ensuring that an appropriate adult is present at any meeting. An appropriate adult is a parent or guardian, a person who has assumed responsibility for the wellbeing of the CHIS or, in their absence, a person who is responsible for the wellbeing of the CHIS and who is over 18, who is neither a member of, nor employed by, the Council.

6.9.5 On no occasion should the use or conduct of a source under 16 years of age be authorised to give information against his/her parent or any person who has parental responsibility for him/her. The processing of information obtained as a result of surveillance should be restricted to specified employees. Only relevant senior managers should have access to the information collected to enable appropriate action to be taken. They must respect the confidentiality of all

information and only disclose the information to other appropriate senior managers where further action is required.

6.9.6 When a CHIS is used, a "Handler" (who can be an Officer of the Council), and who must have received appropriate training, should be designated as having the day to day responsibility for dealing with the CHIS. This responsibility should also extend to the security, safety and welfare of the CHIS. In addition, a "Controller" should be designated to have the general oversight of the use made of the CHIS. These requirements also apply in cases in which the CHIS is an officer of the Council. The officer requesting authorisation for the use of a CHIS must also complete a risk assessment and submit it to the Authorising Officer, together with the authorisation request.

6.10 Test purchases of sales to juveniles

When a young person carries out test purchases at a series of shops/off licences, it is necessary to obtain an authorisation for 'directed' surveillance; it is not necessary to prepare authorisations for each premise to be visited, providing each is identified at the outset but, in all cases, it is necessary to prepare a risk assessment in relation to the young person and to have an adult on hand to observe the test purchase.

7.0 Training

Regular training sessions for Authorising Officers and Investigating Officers will be arranged internally. No officer who has not attended a training session will be permitted to instigate or authorise any application for the use of RIPA powers.

The Council currently has five trained authorising officers –
Chief Executive
Chief Operating Officer
Director of Adults Social Care
Director of Children's Social Care
Director of Public Health

8.0 Review of policy

This Policy and Procedures should be reviewed annually, or sooner if necessary (e.g. in the event of legislation being amended or revoked).

For further guidance please see the relevant Home Office guidance available from The Home Office website https://www.gov.uk/government/organisations/home-office or contact Compliance and Customer Relations.

https://osc.independent.gov.uk/wp-content/uploads/2015/06/OSC-Annual-Report-2014-15-web-accessible-version.pdf

OSC P&G Document
December 2014 - Ver:

covering despatch
letter (Dec 2014).doc