THE REGULATION OF INVESTIGATORY POWERS ACT 2000 (As amended)

(RIPA)

Policy & procedures

5 April 2007 – amended August 2014 (Protection of Freedoms Act 2012)

NORTH NORFOLK DISTRICT COUNCIL

REGULATION OF INVESTIGATORY POWERS ACT 2000 ("RIPA")

POLICY DOCUMENT

1. INTRODUCTION

This Act has significant implications for many areas of work carried out by the Council. The Act does not in any way restrict its operation to specific functions and therefore it is imperative that any officer who might be carrying out surveillance and authorising officers are fully aware of when the need arises for an authorisation to be obtained. This document only sets out the main principles involved around covert surveillance. It must be stressed that any officer requesting authorisation and particularly those persons empowered by the Council to grant authorisations must ensure they receive full and proper training before dealing with any authorisations. However, a considerable amount of what the Council does is OVERT so that the person being investigated is fully aware of the situation. This will never need authorisation.

In 2012 the Act was amended by new legislation – the Protection of Freedoms Act 2012 which provided for judicial approval in relation to certain authorisations and notices under the Regulation of Investigatory Powers.

The information contained within this document has been extracted from the two relevant **Codes of Practice** issued pursuant to section 71 of RIPA 2000, namely the **Covert Surveillance Code (Surveillance Code)** and the **Covert Human Intelligence Sources Code (CHIS Code)**.

There are two types of covert surveillance which might arise in local government, operations, directed surveillance and covert human intelligence sources (ie informants, undercover officers, test purchase officers).

A third type, **intrusive surveillance**, cannot be authorised by local authorities.

Note: Directed surveillance does not include entry on, or interference with, property or wireless telegraphy, nor does it include interception of communications sent by post or by telecommunication systems. These can only be carried out by the Secretary of State, Police or intelligence agencies (depending upon the situation). However, you should not rule out directed surveillance simply because you might overhear telephone conversations, but you cannot deliberately place a device so as to hear such conversations.

2. CONSEQUENCES OF FAILURE TO COMPLY WITH THE LEGISLATION

Article 8 of the Human Rights Convention introduced a new concept in English Law, the right to privacy. To comply with this human right, surveillance, which potentially infringes the right to privacy, should only be done if it is carried out "in accordance with the law". Hence a legal framework to authorise surveillance was required and RIPA was introduced.

RIPA Authorisation provides a lawful authority to carry out covert surveillance provided it is authorised in accordance with the Act. However, a decision not to obtain authorisation does not automatically render the surveillance unlawful. The Act and Codes of Practice are admissible in evidence and so whether authorisation was correctly obtained will be taken into account in any court proceedings about admissibility of evidence and/or human rights challenges. If the Council fails to comply with RIPA it could be ordered to pay compensation either by a court or the ombudsman. An innocent party to collateral intrusion could be entitled to a considerable amount of compensation. It is also possible that evidence gathered via unauthorised surveillance could be ruled inadmissible. This policy document recommends that authorisations are always obtained in accordance with the Act, where appropriate.

3. OFFICE OF SURVEILLANCE COMMISSIONERS

The legislation provides for a Chief Surveillance Commissioner, whose remit it is to provide an independent oversight of the use of the powers contained within Part 2 of the Act, by public authorities.

The OSC will periodically visit the Council for an inspection of our records and protocol. The aims of any inspections are to be as helpful as possible providing feedback on best practice, recurring problem areas and remedies.

4. PROTECTION OF FREEDOMS ACT 2012

4.1 Judicial approval

The Act amends RIPA, requiring local authorities to obtain the approval of a Magistrate for the use of any one of the three covert investigatory techniques available to them under RIPA namely:

- Directed Surveillance,
- deployment of a Covert Human Intelligence Source (CHIS)
- accessing communications data.

4.2 An approval is also required if an authorisation to use such techniques is being renewed. In each case, the role of the Magistrate is to ensure that the correct procedures have been followed and the relevant factors have been taken account of. The new provisions allow the Magistrate, on refusing an approval of an authorisation, to quash that authorisation.

4.3 Directed Surveillance and the Serious Crime Test

Where local authorities wish to use RIPA to authorise Directed Surveillance, this should be confined to cases where the offence under investigation carries a custodial sentence of six months or more (the Serious Crime Test).

4.4 On completion of the Council's internal authorisation procedures – see Para 5.4 below – application must be made to Her Majesty's Courts and Tribunals Service (HMCTS) administration at the magistrates' court to arrange a hearing.

4.5 Court attendance will be required with:

- a counter-signed RIPA authorisation/or notice (for CD authorisations/notices the signatures may be electronic signatures).

- the accompanying judicial application/order form.
- any other relevant reference or supporting material.

5. SURVEILLANCE

The Definition of Surveillance includes:

(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.

5.1 Definition of Directed Surveillance

Very often surveillance is conducted with the intention of that person being unaware that the surveillance is or may be taking place i.e. **covertly**. If observations are made as part of the normal duties of the person or officer involved, which may be termed as **'general observations'** i.e. a planning officer noticing something whilst travelling around the town, is not directed surveillance requiring authorisation. He may consider that as a result of his observation, surveillance action is required. If this surveillance is carried out covertly (i.e. without the person being observed knowing it is or may be taking place) then it is likely to be construed as directed surveillance and would require authorisation under RIPA. If the person subject to surveillance is advised that observations are to be carried out then this is not surveillance that is being done covertly and would fall outside the definition of directed surveillance.

Surveillance does not include obtaining any information revealed while in the presence of the source

Directed Surveillance is defined as surveillances where the following are all true:

- it is covert, but not intrusive surveillance;

- it is conducted for the purposes of a specific investigation or operation;
- it 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);
- it is conducted otherwise than by way of an immediate response to events or circumstances the nature of which is such that it would not be reasonably practicable for an authorisation under Part II of the 2000 Act to be sought.

Thus, 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.

'Private' was defined in case law at the European Court of Human Rights as follows:

'Private life' is a broad term not susceptible to exhaustive definition. Aspects such as gender identification, name, sexual orientation and sexual life are important elements of the personal sphere protected by Article 8 human rights Act. The article also protects a right to identity and personal development, and the right to establish and develop relationships with other human beings and the outside world, and it may include activities of a professional or business nature. There is, therefore, a zone of interaction of a person with others, even in a public context, which may fall within the scope of 'private life'. It cannot therefore be excluded that a person's private life may be concerned in measures affected outside a person's home or private premises. A person's reasonable expectation as to privacy is a significant though not necessarily conclusive factor.

P.G. and J.H. v. the United Kingdom, no. 44787/98, §56 & 57, ECHR 2001-IX, with further references)

- is conducted in such a way as to obtain a detailed picture about the manner in which that person conducts their private life, activities and associations.

Directed surveillance does not include any type of covert surveillance carried out in residential properties or in private vehicles. This is intrusive surveillance that local authorities cannot authorise.

5.2 Intrusive Surveillance

Is defined as covert surveillance that:

- is carried out in relation to anything taking place on any residential premises or in 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.
- This does not include the use of overt CCTV cameras positioned in their normal position where the public are aware that the systems are in use for their own protection and to prevent crime.

Local authorities cannot authorise intrusive surveillance.

5.3 Other Surveillances

Similarly, the District Council cannot conduct entry on, or interference with, property or with wireless telegraphy (known as “property interference”).

5.4 Authorisation Forms

The amendments in the Protection of Freedoms Act 2012 mean that local authority authorisations and notices under RIPA for the use of particular covert techniques can only be given effect once an order approving the authorisation or notice has been granted by a magistrate as detailed in para 4.1 above.

All surveillance should be authorised by an appropriate person as prescribed for the purposes, under Section 30 of RIPA and The Regulation of Investigatory Powers (Directed Surveillance and Covert Human Intelligence Sources) Order 2003, using the appropriate forms, which are: -

- **Application** for authority for directed surveillance; which requests specific information enabling the authorising officer to consider the request. The initial application should be for a period that is compatible with the objectives of the surveillance. The maximum period for any authorisation is 3 months and you must either cancel or renew it *before* it expires. However, all authorisations must be cancelled eventually (some may be renewed a number of times but still must be cancelled eventually)

- **Renewal** of directed surveillance authorisation; for use when it is considered necessary for the authorisation to continue.

- **Cancellation** of directed surveillance authorisation; for use when the directed surveillance no longer meets the criteria for authorisation. The cancellation will normally be authorised by the officer who last renewed or authorised the surveillance. **All operations must be finalised with a cancellation form regardless of the conclusion**. There is no requirement for the magistrates court to consider cancellations.

These forms are attached. They will no doubt be reviewed or updated over time and this can be checked on the home office web site, if necessary (www.homeoffice.gov.uk/crimpol/crimeduc/regulation/forms/index.html).

5.5 Collateral Intrusion

If at any stage during the surveillance it becomes apparent that there is unexpected interference into the privacy of persons who are not the original subject of the investigation (this is called collateral intrusion) then this information and any other matters that arise of a similar sensitive nature, should be brought to the Authorising Officer's attention. This will enable the Authorising Officer to reconsider the original authorisation taking into consideration the new information. The Authorising Officer should particularly bear in mind the proportionality of the surveillance in this situation.

5.6 Authorising Officers – who can make a decision?

Officers Authorised to Approve Applications For Directed Surveillance and CHIS

Officer	Name	Contact Details
Nick Baker	Corporate Director	01263 516221 nick.baker@north-norfolk.gov.uk
Stephen Hems	Head of Environmental Health	01263 516182 stephen.hems@north-norfolk.gov.uk

Authorisation will normally be granted by Steve Hems, Head of Environmental Health. As SRO, Nick Baker, Corporate Director, may also authorise but best practice is for the SRO to only have an overseeing role in authorisation. Such authorisation is for directed surveillance or the use of covert human intelligence sources as defined in Article 4 of The Regulation of Investigatory Powers (Directed Surveillance and Covert Human Intelligence Sources) Order 2003.

Other officers will be authorised to approve applications on Directed Surveillance as deemed necessary by CLT.

Any officer authorising such decisions must ensure that he or she is properly trained so that the decision is made in accordance with the law. It is important that the person seeking authorisation and the Authorising Officer ensures that the decision to take (and it is recommended not to take) action is properly documented with full reasons. Comments should be put in the necessity and proportionality box in the application form even if these are just “I agree”. It is also important to note that the authorising officer’s job does not stop should s/he agree to authorisation. That person must keep the investigation under review, particularly if information may be obtained about someone other than the target of the surveillance (collateral intrusion). In all surveillance the risks should also be assessed properly and kept under review. So that there is a proper review system officers should record the date when the authorisation should be reviewed. Whilst this can be the full 3 months permitted the review will invariably be a much shorter period.

5.7 What the Authorising Officer must take into account?

1. Authorisation shall not be granted unless it is believed **necessary** for the **purposes of preventing or detecting a crime or preventing disorder**.

2. Ensure compliance with the data protection requirements and any other relevant codes of practice and ensure that any confidential material obtained during the course of the surveillance is securely maintained. Confidential material includes matters subject to legal privilege, confidential personal information and confidential journalistic material. These terms are explained further in the Surveillance Code. Where it is likely that the surveillance will result in the acquisition of such information, the authorising officer will discuss with the SRO before authorisation will be given.

3. Consider the impact of **collateral intrusion** relating to persons other than the subject of the surveillance. (see explanation above).

4. **Proportionate** to what the surveillance seeks to achieve. In other words, is the Council over using its resources in order to get the result?

   The Authorising Officer must

   a. balance the size and scope of the operation against the gravity and extent of the perceived mischief

   b. explain how and why the methods to be adopted will cause the least possible intrusion on the target and others

   c. ensure that the activity is an appropriate use of the legislation and the only reasonable way, having considered all others, of obtaining the necessary result

   d. evidence what other methods had been considered and why they were not implemented.

   The Authorising Officer should set out why he is satisfied (RIP(S)A) or why s/he believes the surveillance proposed is necessary and proportionate. A bare assertion is insufficient.

5. Special care needs to be given in relation to **joint operations** with other agencies and where the Council employs an agent to carry out investigations on its behalf.

6. Legal Advice. It is recommended that legal advice is sought from the Council's legal advisors on any proposed RIPA surveillance prior to authorisation.

5.8 Central Records

Each Authority should maintain a central record (register) relating to all authorisations, giving details of what the authorisation was for and the dates during which surveillance has been carried out.

A full list of the matters to be recorded can be found in paragraph 2.14 – 2.15 of the **Surveillance Code**. Paragraphs 2.16 - 2.18 give details concerning the retention and destruction of such documents. See Appendix 4 for a blank copy of the Central Record, to see the information required.

5.9 Emergency Situations

An emergency situation would only arise if the time that would elapse before the authorising officer was available to grant the authorisation would, in the judgement of the person giving the authorisation, be likely to endanger life or jeopardise the investigation or operation for which the authorisation was being given. An authorisation is not to be regarded as urgent where the need for an authorisation has been neglected or the urgency is of the authorising officer's or applicant's own making. These rules must not be used where there has been a failure to obtain authority at the appropriate time.

Where it is not reasonably practicable for an authorisation in writing under this part to be sought because it is urgent then the authorisation can be granted **orally**. In this situation the decision must be recorded in writing at the earliest opportunity by the person seeking authority and endorsed by the Authorising Officer. Details of urgency should also be given.

In practice, given the nature of the Council's statutory responsibilities it is extremely unlikely to envisage circumstances where such an emergency situation might arise.

6. COVERT HUMAN INTELLIGENCE SOURCE

6.1 Introduction

This does not apply to circumstances where members of the public **volunteer** information to the Council. However, someone may become a CHIS as a result of supplying information to the Council. A specific issue arises as to whether someone becomes a CHIS because the Council issues them with diary/monitoring sheets and asks them to tell them of any further problems (ie anti-social behaviour cases). This does not require specific authorisation unless a personal relationship between the alleged perpetrator and the complainant/witness exists or is cultivated (see below). Any authorisation can be sought on the same form as for directed surveillance.

6.2 Definition of a CHIS

A person is a covert human intelligence source if:

(a) He establishes or maintains a **personal or other relationship** with a person for the **covert** purpose of facilitating the doing of anything falling within paragraph b) or c),

(b) He covertly uses such a relationship to obtain or to provide access to any information to another person; or

(c) He covertly discloses information obtained by the use of such a relationship or as a consequence of the existence of such a relationship

(d) The relationship is used covertly if and only if it is conducted in a manner calculated to ensure that one party is unaware of its purpose.

6.3 What the Authorising officer must take into account

1. Must believe that the authorisation is **necessary** for the purposes of preventing and detecting crime or of preventing disorder

2. It is **proportionate** to what it seeks to achieve & appropriate arrangements for managing the source,

3. Should take into account the risk of collateral intrusion,

4. Ensure particular care is taken concerning **confidential material,**

5. Any adverse impact upon the **community confidence,**

6. Assess any **risk to the source.**

7. Legal advice obtained from the Council's legal advisors.

Sometimes authorisation is needed in the process of cultivating the source where this would infringe the privacy of the source. The cultivation process itself may require authorisation if it involves directed surveillance, for example.

6.4 Authorisations

These work in a similar way to directed surveillance and must be authorised in **writing**, **orally in emergency** situations. The use of **vulnerable** sources should only take place in exceptional circumstances. **Juveniles** can never be used as sources against their own parents but can be used subject to special safeguards (see 6.8 below).

Information to be given in applications for authorisation: -

1. Details of the purpose for which the source will be deployed.

2. The grounds on which authorisation is sought (i.e. detection of crime).

3. Where a specific investigation is involved details of that investigation.

4. Details of what the source will be tasked to do.

5. Details of the level of authority required.

6. Details of potential collateral intrusion.

7. Details of any confidential material that might be obtained as a consequence of the authorisation.

Particulars to be contained in records

The following matters are specified as being particulars of which must be included in the records relating to each source:

(a) the identity of the source;

(b) the identity, where known, used by the source

(c) any relevant investigating authority other than the authority maintaining the records;

(d) the means by which the source is referred to within each relevant investigating authority;

(e) any other significant information connected with the security and welfare of the source;

(f) any confirmation made by a person granting or renewing an authorisation for the conduct or use of a source that the information in paragraph (d) has been considered and that any identified risks to the security and welfare of the source have where appropriate been properly explained to and understood by the source;

(g) the date when, and the circumstances in which, the source was recruited;

(h) the identities of the persons who, in relation to the source, are discharging or have discharged the functions mentioned in section 29(5)(a) to (c) of the 2000 Act or in any order made by the Secretary of State under section 29(2)(c);

(i) the periods during which those persons have discharged those responsibilities;

(j) the tasks given to the source and the demands made of him in relation to his activities as a source;

(k) all contacts or communications between the source and a person acting on behalf of any relevant investigating authority;

(l) the information obtained by each relevant investigating authority by the conduct or use of the source;

(m) any dissemination by that authority of information obtained in that way; and

(n) in the case of a source who is not an undercover operative, every payment, benefit or reward and every offer of a payment, benefit or reward that is made or provided by or on behalf of any relevant investigating authority in respect of the source's activities for the benefit of that or any other relevant investigating authority.

6.5 Duration of authorisation

A written authorisation (except a juvenile source) is valid for 12 months from the date it took effect but oral authorisations cease to have effect 24 hours after being granted.

6.6 Renewals

A review should be carried out and the authorising officer satisfied that the conditions for authorisation continue to be met before the authorisation is renewed for a further period. Provided conditions continue to be met authorisation can be renewed more than once. The renewal extends the time from the time when the authorisation would expire (but for the renewal) so the renewal decision should be taken shortly before expiry of the authorisation.

6.7 Cancellations

Authorisations should be cancelled where the conditions justifying authorisation are no longer satisfied. The authorising officer should do this in writing although it is suggested that the officer seeking authorisation should also seek cancellation where s/he becomes aware that the conditions are no longer satisfied. There is a standard form for recording this. Although some

authorisations will be renewed on a number of occasions, **every authorisation must be cancelled at the end of the surveillance operation.**

When cancelling an authorisation, an Authorising Officer must ensure that proper arrangements have been made for the activity's discontinuance, including the removal of technical equipment and directions for the management of the product.

6.8 Juvenile CHIS

Special safeguards also apply to the use or conduct of juvenile sources; that is sources under the age of 18 years. Authorisation will not normally be granted.

On no occasion should the use or conduct of a source under 16 years of age be authorised to give information against his parents or any person who has parental responsibility for him.

In other cases, authorisations should not be granted unless the special provisions contained within The Regulation of Investigatory Powers (Juveniles) Order 2000 are satisfied.

The use of sources under 16 is dependent on there being an appropriate adult present at any meeting with the Council.

Appropriate adult is defined as:

(a) the parent or guardian of the source;

(b) any other person who has for the time being assumed responsibility for his welfare; or

(c) where no person falling within (a) or (b) is available, any responsible person aged eighteen or over who is neither a member of nor employed by any relevant investigatory authority.

The Order states that at all times there must be a person within the investigating authority who has responsibility for ensuring that the appropriate adult is present at the meetings.

The duration of such an authorisation is **one month** instead of twelve months.

Restrictions are also imposed on the use of any source under the age of 18. In particular, a person in the investigating authority must make a risk assessment in order to assess the nature and magnitude of any risk of physical injury or psychological distress involved in the proposed course of action, and the person granting the authorisation must be satisfied that the risks are justified and that the source understands the risk and that he has given consideration to the particular relationship, if any, between the source and the target of the authorisation.

7. RECORD KEEPING

This must be done in such a way as to preserve the confidentiality of the source. The authorising officer must not grant an authorisation unless satisfied that there are arrangements in place to ensure that someone has responsibility at all time for maintaining a record of the use made of the source. This should be an officer within the client department and they should record a number of matters (for example, the identity of the source, identities used by the source, how the authority of refers to the source, information about the source's security and welfare, how recruited etc). A full list of the matters to be recorded can be found in paragraph 2.13 – 2.16 of the **CHIS Code**. Paragraphs 2.17 - 2.19 give details concerning the retention and destruction of such documents