Appendix 1

Exeter City Council

The Covert Surveillance and Covert Human Intelligence Source Procedures

1. Introduction

1.1 The Regulation of Investigatory Powers Act 2000 (RIPA) imposes various provisions regarding the:

- interception of communications
- acquisition and disclosure of data relating to communications
- carrying out surveillance
- use of Covert Human Intelligence Sources (CHIS)
- acquisition of various electronic data

1.2 The aim of RIPA is to ensure that such activities are carried out in accordance with the law and are therefore less vulnerable to challenge under the Human Rights Act 1998

1.3 Council officers who undertake directed covert surveillance or use Covert Human Intelligence Sources (collectively referred to as 'surveillance operations') must be familiar with these procedures.

1.4 Compliance with the RIPA provisions is monitored and periodic visits made by the Office of the Surveillance Commissioner (OSC). Officers must therefore ensure that they comply with these procedures at all times, whether or not it is intended to use any information from a surveillance operation as evidence in court or for other proceedings

1.5 The Home Office has issued codes of practice for the use of covert surveillance and of CHIS. The codes are published on the RIPA intranet page.

2. Definition of RIPA terms

2.1 *Collateral Intrusion* – is the risk of interference with, or intrusion into, the privacy of any other person or persons other than the subject of the proposed surveillance.

2.2 *Confidential Material* refers to:

- matters subject to legal privilege
- confidential personal information relating to a person's physical or mental health, spiritual counselling or other assistance being given or oral or written information arising in the course of any trade, business etc, that is held subject to an undertaking of confidence or a restriction on disclosure or obligation of secrecy contained in legislation
- confidential journalistic material being material acquired or created for the purposes of journalism

2.3 *Covert Human Intelligence Source* (CHIS) - is the use of a person to establish or maintain a personal or other relationship with another person in order to:

- obtain information or to provide access to any information to another person, or
- disclose information obtained through the relationship

in a manner that ensures the other party is unaware of what is being undertaken

2.4 *Covert Surveillance* - is surveillance that is carried out in a way that the subject of the surveillance is unaware that it is or may be taking place

2.5 *Directed Covert Surveillance* - surveillance is directed surveillance if all of the following apply:

- 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

2.6 *Intrusive Covert Surveillance* - is covert surveillance that:

- is carried out in relation to anything taking place on a residential premise or in any private vehicle
- involves the presence of an individual on the premises or in the vehicle or is carried out by means of a surveillance device

Note: Intrusive Covert Surveillance cannot be authorised or undertaken as the Council does not have the necessary legal powers

2.7 *Necessity* - is the requirement to consider why use of covert surveillance is needed, and ensuring that the request is in fact in connection with preventing and detecting crime or preventing disorder

2.8 *Officer* - is a person employed by Exeter City Council

2.9 *Proportionality* – is the requirement that consideration is given to whether the proposed covert surveillance is:

- proportional to the 'mischief' under investigation
- proportional to the degree of anticipated intrusion on the target and others
- the only option, other overt means having been considered and discounted

2.10 *Surveillance* – includes:

- monitoring, observing or listening to persons, their movements, their conversations or their other activities or communications
- recording anything monitored, observed or listened to in the course of surveillance
- surveillance by or with the assistance of any surveillance device

2.11 *Surveillance Device* - is any apparatus designed or adapted for use in surveillance

3. Activities subject to RIPA

3.1 The following activities are subject to RIPA and therefore require authorisation:

a) use of *Directed Covert Surveillance* - the surveillance of an individual with a view to obtaining information without their knowledge

b) use of a *CHIS* - using a person to interact with another person in order to obtain information about them without that person knowing. The CHIS may be an officer or a third party.

3.2 **Note**: A surveillance operation can only be authorised if it is for the purposes of preventing and detecting crime or preventing disorder

4. Activities not affected by the Act

4.1 RIPA does not apply to surveillance that is not covert, for example:

- the use of overt CCTV surveillance systems. However, these are subject to other controls (e.g. Data Protection Act 1998).
- general observations undertaken by an officer in the normal performance of their duties that does involve the systematic surveillance of an individual will not usually be regulated by RIPA
- surveillance undertaken where the subject concerned is aware that it is or may be taking place

5. The need for authorisation

5.1 Whenever there is an intention to undertake directed covert surveillance or use a CHIS then appropriate authorisation **must** first be obtained

6. Officers who can grant an authorisation

6.1 Authorisation can only be granted by one of the following:

- Assistant Director Finance

- Corporate Manager Legal

6.2 **Note**: In normal circumstances, if one of the above authorising officers is directly involved in undertaking an investigation, then they must not give authority to themselves. An exception is where the matter is sufficiently urgent that it prevents the officer from obtaining authority from one of the other authorising officers.

7. Covert surveillance and Covert Human Intelligence Sources (CHIS) authorisations

7.1 **Application**

a) An application for directed surveillance or CHIS must be made in writing on the appropriate form, unless the situation is urgent (please see 8 below). These are published on the RIPA intranet page.

b) All relevant parts of the application form must be completed by the officer seeking the authorisation, in particular information must be provided that:

- explains the action that is being authorised, including any premises or vehicles involved
- identifies, where known, the subject of the surveillance operation
- specifies the grounds on which authorisation is sought
- explains why the surveillance operation is necessary
- explains why the surveillance operation is considered 'proportionate', a concept arising from the Human Rights Act, and applies to both the surveillance operation itself and the length of time it will continue for. Proportionality covers necessity and requires consideration to be given to assessing the scope of the surveillance operation to the actual 'mischief' concerned
- identifies what information is desired from the surveillance
- specifically addresses the likelihood and extent of intrusion or interference with the privacy of other persons other than the subject of the surveillance operation
- assesses the likelihood of acquiring any confidential material
- identifies any surveillance device that is proposed to be used

c) **In the case of a CHIS, the information must also include**:

- information relating to the intended CHIS
- the purpose for which the CHIS will be used
- the nature of what the CHIS will be assigned to undertake

d) The authorising officer must examine all of the information on the application form, and before authorising must consider:

- is the requested surveillance lawful
- is the surveillance proportionate
- Is the surveillance operation necessary on the ground shown (i.e. preventing and detecting crime or preventing disorder)
- what the risk of collateral intrusion is
- what the likelihood of obtaining confidential material is. (Note: where confidential material may be obtained then authority for the surveillance operation and possibility of obtaining confidential material must be given by the Chief Executive or by whoever deputises for him/her when they are unavailable)
- is the use of any surveillance device acceptable

Note: At the time of signing, the authorising officer should contact the RIPA monitoring officer in order to obtain the consecutive '*Unique Reference Number*' that needs to be entered onto the form

e) **Where surveillance involves a CHIS then there are the following additional issues:**

- special consideration must be given to any risks that the CHIS may face whilst they are undertaking the activities proposed
- vulnerable individuals must not be used as a CHIS unless authorised by the Chief Executive or by whoever deputises for the CX when he is unavailable
- the use of a juvenile as a CHIS (i.e. a person under 18 years of age) requires special consideration. Under no circumstance should a CHIS under 16 years of age be authorised to give information against his/her parents. In any event, a juvenile must not be used as a CHIS

unless authorised by the Chief Executive or by whoever deputises for him/her when they are unavailable.

f) At the time of authorisation, the authorising officer must set a period or date in which the authorisation must be reviewed (e.g. within 1 month). However, where there is potential access to confidential information, collateral intrusion or use of vulnerable individuals/juveniles, then more frequent reviews must be undertaken

g) The applicant/officer undertaking the surveillance should take a photocopy of the authorised form and keep it with their surveillance notes, documents, record, etc. for reference. The original authorised application form should be immediately sent to the RIPA monitoring officer (the Head of Audit) who maintains the central record.

h) **Note**: A directed covert surveillance authorisation ceases to have effect after 3 months from the day that it took effect. Urgent authorisations cease to have effect after 72 hours from the time when the authorisation was granted

i) **Note**: A CHIS authorisation ceases to have effect after 12 months from the day that it took effect unless the CHIS is a juvenile in which case it will only last 1 month. Urgent authorisations cease to have effect after 72 hours from the time when the authorisation was granted

j) Once an investigation has been completed, all written details associated with it (including the original authorisation, renewal, etc.) must be kept for 6 years in a secure location, where they can be easily found should an authorised person require to examine them

7.2 **Review**

a) The officer who applied for the authorisation (or other suitably experienced officer) must review the application in accordance with the period or date specified by the authorising officer (see 7.1g). The forms are published on the RIPA intranet page.

b) Details of the review should be recorded in writing on the form, and the authorising officer must either approve the application or cancel the surveillance. However, before doing so the authorising officer must consider the continuing necessity and proportionality of the application. The officer undertaking the surveillance or carrying out the review should take a photocopy of the form and keep it for reference and send the original to the RIPA monitoring officer immediately for entering onto the central record.

c) The officer undertaking the surveillance or carrying out the review must promptly notify the authorising officer if an investigation unexpectedly interferes with the privacy of individuals who are not covered by the authorisation. Consideration should at the same time be given as to whether a further authorisation is required.

7.3 **Renewal**

a) A request to renew the authorisation should be made prior to the existing authorisation ceasing, and should normally only be made close to the cessation of the existing authorisation. The forms are published on the RIPA intranet page.

b) An authorising officer can renew an authorisation in writing (whether originally given orally or in writing) for a further period of 3 months. However, before doing so the authorising officer must consider the continuing necessity and proportionality of the application. Only in the most exceptional circumstances would it be considered appropriate to renew an authorisation orally.

c) The request for renewal should contain the following information:

- whether this is the first renewal, or if not, when the authorisation were previously renewed
- the details required for the original authorisation as they apply at the time of the renewal
- any significant changes to the information
- the reasons why continued surveillance is necessary and proportionate

- the content and value to the investigation of information so far obtained
- an estimate of the length of time that further surveillance is necessary

d) If the authorising officer decides the request should not be granted then the reasons should be recorded on the renewal form and show clearly why the renewal was refused

e) The officer undertaking the surveillance should take a photocopy of the renewal form (even if refused) and keep it for reference and send the original to the RIPA monitoring officer immediately for entering onto the central record.

f) An authorisation must be either renewed or cancelled (once the specific surveillance is complete or about to expire) as it does not lapse with time

7.4 **Cancellation**

a) Each approved authorisation must be formally cancelled unless it is renewed. The forms are published on the RIPA intranet page.

b) The authorisation must be cancelled where the directed covert surveillance has achieved its purpose or no longer meets the authorisation. The form must be signed by an authorised officer who needs to record on the form the time and date when the authorisation was cancelled

c) The officer undertaking the surveillance should take a photocopy of the cancellation form and keep it for reference and send the original to the RIPA monitoring officer immediately for entering onto the central record.

8 Urgent authorisations

8.1 A situation should only be regarded as urgent if, in the time that would elapse to enable normal procedure to be followed, it could endanger life or jeopardise the investigation
Note: Before applying for such, ensure that the surveillance is not already covered by the immediate response provision in the Regulation of Investigatory Powers Act 2000 section 26.2.c

8.2 In normal circumstances, surveillance must not be undertaken without written authorisation. If the situation is considered urgent so that an application form cannot be completed, then an oral authorisation may be given. In such cases, the officer seeking authority should record in writing as soon as possible a statement of the authorisation given. Furthermore, within 2 working days of the authority being given all of the details that would normally have been provided on an application form should be completed in writing and the original copy sent to the RIPA monitoring officer with a summary of the oral authorisation that was given

9 Confidential Material

9.1 Every officer involved in a surveillance operation should ensure that they are familiar with what is meant by confidential material. If at any time during surveillance an officer is unsure whether confidential information has been obtained then they should consult the Corporate Manager Legal as soon as possible and ensure that further information is not obtained until the situation is clarified.

10 Record keeping

10.1 The officer carrying out surveillance must maintain an adequate log/record as these might be needed in the event of subsequent proceedings.

10.2 Any alterations in the log/record should be crossed through with a single line, initialled and the correct information written to the side, correction fluid must not be used. No blank lines should be left where additional information could later be written in at a later date

10.3 The log/records should be signed as true statements and held with the surveillance notes, documents, record, copies of the authorised forms, etc. securely for six years

11 The RIPA monitoring officer's role

11.1 The RIPA monitoring officer is responsible for:

a) maintaining the central record of RIPA authorisations, reviews, renewals and cancellations and keeping copies of all authorisations for at least three years from the ending of the authorisation
Note: Specific records must be kept of any:
- urgent authorisations
- authorisations relating to confidential material
- authorisations for the conduct or use of a vulnerable individual or juvenile as a CHIS

and that such cases must be brought to the attention of the OSC inspector when he/she visits.

b) oversight of the Council's RIPA process.

c) monitoring the day-to-day operation of RIPA and checking that authorisations are in compliance with legislation; and with relevant codes of practice, procedures and guidance.

d) raising awareness of RIPA within the Council, and organising a RIPA training programme

11.2 The RIPA monitoring officer will undertake an annual review of the operation of these procedures, and prepare reports referred to at 13.1 and 13.2 below.

12 The senior responsible officer's role

12.1 The 2010 revised code of practice for directed surveillance and CHIS under RIPA considers it good practice for every public authority for a senior responsible officer (SRO) to be made responsible for:
- the integrity of the process in place within the public authority for the management of CHIS;
- compliance with Part II of the Act and with the Codes;
- oversight of the reporting of errors to the relevant oversight Commissioner and the identification of both the cause(s) of errors and the implementation of processes to minimise repetition of errors;
- engagement with the OSC inspectors when they conduct their inspections, where applicable; and
- where necessary, oversight of the implementation of post-inspection action plans approved by the relevant oversight Commissioner

12.2 The SRO is responsible for ensuring that all authorising officers are of an appropriate standard in light of any recommendations in the OSC's inspection reports, and addressing any concerns about the standards of authorising officers.

12.3 The SRO should be a member of the corporate leadership team

13 Councillors

13.1 Councillors are responsible for reviewing the use of RIPA and setting the policy once a year.

13.2 Quarterly reports are made on the use of RIPA to Councillors who are responsible for ensuring that RIPA is being used consistently with the Council's policy, and that the policy remains fit-for-purpose. However, Councillors must not be involved in making decisions on specific RIPA authorisations.

14 Complaints

14.1 An independent tribunal has been established to investigate RIPA complaints, information about the complaints procedure is obtainable from:
Investigatory Powers Tribunal
PO Box 33220
London
SWLH 9ZQ

Telephone 020 035 3711 Website http://www.ipt-uk.com/