REGULATION OF INVESTIGATORY POWERS ACT 2000

POLICY
and
CODE OF PRACTICE

Revised October 2023

Sheffield City Council

SHEFFIELD CITY COUNCIL

REGULATION OF INVESTIGATORY POWERS ACT 2000

Council Policy Document

Code of Practice on Directed Surveillance and Covert Human Intelligence Sources

Appendix 1 **Flowcharts**

Appendix 2 **Duties of Authorising Officers**

Appendix 3 **Duties of Officers in charge of investigations**

Appendix 4 **Management of Covert Human Intelligence Sources**

Appendix 5 **List of Authorising Officers**

REGULATION OF INVESTIGATORY POWERS ACT 2000

COUNCIL POLICY DOCUMENT

Introduction

The Regulation of Investigatory Powers Act 2000 (RIPA) established a statutory framework for the regulation of covert surveillance by a number of bodies, including all local authorities.

The Act is designed as a mechanism to provide the correct balance between an individual's rights to privacy and the proper use of data and surveillance, having due regard to human rights, as defined in the Human Rights Act, 1998.

The gathering of evidence may sometimes involve the use of covert surveillance measures which impinge on an individual's privacy. Where this is likely to happen, the surveillance must be subject to an authorisation, review and cancellation procedure to ensure that it is lawful. Part II of the Act also provides for an authorisation mechanism which Authorities undertaking covert directed surveillance, or the use of covert human intelligence sources, must use. In addition, the Home Office has issued Codes of Practice on the conduct of Covert Surveillance and the use of Covert Human Intelligence Sources (CHIS).

This document represents Sheffield City Council's Policy and Code of Practice on Directed Surveillance and the use of Covert Human Intelligence Sources.

Definitions

"surveillance" , as defined in Section 48 of RIPA includes the monitoring, observing, listening recording, etc of the movements, activities or communications of persons.

"covert surveillance" is conducted without the knowledge of the subject of the surveillance.

"directed surveillance" is covert (but not intrusive) surveillance which is part of a specific investigation and which is likely to gather private information about any person.

"intrusive surveillance" is covert surveillance that relates to what is taking place in any residential premises or in any private vehicle or place for legal consultation and involves someone on the premises or in the vehicle or is carried out by means of a surveillance device.

"covert human intelligence sources" are people who form a relationship with someone else with the intention of covertly obtaining information, e.g. undercover agents or informants.

(NOTE: These definitions are summaries of those contained in the Regulation of Investigatory Powers Act, 2000 (RIPA), which always take precedence. Further details of the definitions are set out in the Code of Practice)

Directed Surveillance

The Regulation of Investigatory Powers Act 2000 (RIPA) applies in respect of directed surveillance, which is defined as covert surveillance which is undertaken:

- for the purpose of a specific investigation or a specific operation;
- in such a manner as is likely to result in the obtaining of private information about a person (e.g. information about their private or family life) whether specifically identified for the purposes of the specific investigation or operation or not; and
- otherwise than by way of an immediate response to events or circumstances, which would make it not reasonably practicable to seek an authorisation.

The Act regulates the way in which Local Authorities carry out directed surveillance (see Code of Practice) and sets a legal framework for any conduct carried out in accordance with the Act.

Policy Statement

Great care must be taken at all times to make sure that the use of surveillance is lawful, necessary and proportionate to the desired outcome of that surveillance.

The Council will not use covert surveillance:

- unless lawful
- unless it is necessary to do so.
- in a disproportionate way.

The Council will when using directed surveillance:

- do so with due consideration of human rights issues.
- properly investigate any complaints made about its use.
- actively monitor its use.
- observe the appropriate law and Home Office Codes of Practice.
- ensure that staff (and contractors) are properly trained.

The Council will not, in the normal course of any covert surveillance activity, use Covert Human Intelligence Sources. If there appears to be a need to employ such sources, the application must be authorised by either the Chief Executive or the Director of Legal and Governance. The appropriate Home Office Code of Practice and law will then be followed.

The Council will not carry out intrusive surveillance within the meaning of the The Regulation of Investigatory Powers Act, 2000.

The Council will establish and maintain a Code of Practice on the use of directed surveillance. This will be based on the Government approved Code and all staff and contractors who may use directed surveillance will be expected to abide by it.

The Council will produce forms for use in authorising, etc, surveillance operations.

The Council will maintain central records of all directed surveillance operations which it undertakes and will monitor the quality of authorisation forms.

Responsibilities

Overall responsibility for each directed surveillance operation will lie with the officer in charge of the operation.

Officers who authorise directed surveillance are responsible for granting, reviewing, renewing and cancelling authorisations.

The Council's Senior Responsible Officer (SRO) is Claire Taylor, Chief Operating Officer, who is responsible for:

- the integrity of the RIPA process within the Council;
- compliance with RIPA and its regulatory framework;
- engagement with the Office of Surveillance Commissioners and Inspectors when they conduct inspections;
- overseeing the implementation of any recommendations made by the OSC; and
- ensuring that all Authorising Officers are of the appropriate standard.

The Council's RIPA Co-ordinating Officer is Patrick Chisholm, Service Manager, Legal Services, who is responsible for all aspects of the Council's involvement with RIPA including:

- monitoring the quality of authorisation forms;
- updating the Council's Policy and Code of Practice and Forms;
- acting as the contact point for the OSC;
- training and awareness raising;
- providing advice to those involved in covert surveillance; and

- ensuring that all areas which may undertake directed surveillance operations, are familiar with the RIPA legislation, Codes of Practice and the Council's Policy and Code of Practice, including the provision of training.

The Council's RIPA Record Keeper is Sarah Green, Senior Information Management Officer / Data Protection Officer, who is responsible for:

- maintaining the Central Record of Authorisations;

- updating the statistics provided on the Council's website; and

- providing the RIPA Co-ordinating Officer with statistics as required.

The Council's Internal Audit service may periodically review this area of work.

In cases where the Council's equipment or premises are used by the Police for the purposes of their investigations, the Police will be responsible for obtaining the necessary authorisations under the Act. Council officers or the Council's agents should ensure that an appropriate authorisation has been obtained. In cases where joint operations are undertaken, the lead authority should obtain the authorisation.

Member Involvement

Elected Members are kept informed of the Council's covert surveillance activities by means of reports to either the Committee with responsibility for finance or audit or the Information Governance Board.

Non-Compliance with this Policy and Code of Practice

Whilst every effort will be made to fully comply with this Policy and the Code of Practice any failure to do so shall not, on its own, render any action taken unlawful or indicate disapproval by the Council.

SHEFFIELD CITY COUNCIL

CODE OF PRACTICE ON DIRECTED SURVEILLANCE AND COVERT HUMAN INTELLIGENCE SOURCES

The Home Office has issued Codes of Practice which give guidance on Covert Surveillance and the use or conduct of Covert Human Intelligence Sources. They are available on the following website https://www.gov.uk/government/collections/ripa-codes together with the relevant legislation.

This Code of Practice applies to authorisations for Directed Surveillance and the use of Covert Human Intelligence Sources by the Sheffield City Council. The following areas of work could be involved:-

- Environmental Regulation (Trading Standards and Environmental Protection)
- Corporate Resources (Internal Audit and Human Resources)
- Planning
- Licensing
- Children and Young People
- Litigation
- CCTV
- Social media

A copy of the Code is available for inspection at First Stop Reception or on the Council's website at www.sheffield.gov.uk . Council employees can access the Code and forms on the Council's Intranet.

Complaints concerning alleged breaches of the Code should be made to:-

Claire Taylor,
Chief Operating Officer
Sheffield City Council,
Town Hall,
Sheffield S1 2HH

In addition, the complainant must be made aware of the Independent Tribunal established under the Act, who have the power to investigate and decide on cases within its jurisdiction. They can be contacted on:-

The Investigatory Powers Tribunal
PO Box 33220
London SW1H 9ZQ

1. INTRODUCTION

1.1 This Act came into effect in 2000 and, amongst other things, it provides a framework within which Directed Surveillance can take place with due regard to human rights.

1.2 Authorisations for Directed Surveillance can only be given for the purpose of preventing or detecting crime where the offence is punishable by a maximum term of at least 6 months' imprisonment or relates to the underage sale of alcohol or tobacco.

1.3 The material obtained through Directed Surveillance may be used as evidence in criminal proceedings. The proper authorisation of surveillance should ensure the admissibility of such evidence under the common law, Section 78 of the Police and Criminal Evidence Act 1984 and the Human Rights Act 1998.

1.4 The Council will not use Directed Surveillance:-

- Unless it is necessary to do so.
- In a disproportionate way.

1.5 In general, the Council will not use Covert Human Intelligence Sources. If there appears to be a need to employ them, the application must be authorised by either the **Chief Executive** or the General Counsel, **Legal Services and following advice from the SRO.**

1.6 Officers who authorise Directed Surveillance are responsible for granting, reviewing and cancelling authorisations.

1.7 Corporate responsibility for monitoring the use of covert surveillance rests with the Chief Operating Officer, who is the designated Senior Responsible Officer.

1.8 The Internal Audit Service may periodically review this area of work.

1.9 Inspections on the use of this Code of Practice will be carried out by Inspectors of the Investigatory Powers Commissioners Office (IPCO).

2. DEFINITIONS

2.1 **Directed Surveillance** is defined in Section 26(2) of the 2000 Act as surveillance which is covert, but not intrusive, and is undertaken:-

- For a specific investigation or a specific operation;
- In a manner <u>likely</u> to result in the obtaining of private information about a person (i.e. information about their

private or family life) whether specifically identified for the purposes of the specific investigation or operation or not;

and

- Otherwise than by way of an immediate response to events or circumstances which would make it not reasonably practicable to seek an authorisation.

2.2 Directed Surveillance does not include covert surveillance carried out by way of an immediate response to events or circumstances which, by their very nature, could not have been foreseen. For example, a police officer would not require an authorisation to conceal himself and observe a suspicious person that he came across in the course of a patrol.

2.3 Where surveillance is carried out by a device designed or adapted principally for the purpose of providing information about the location of a vehicle, the activity is directed surveillance and **should be** authorised accordingly.

2.4 Directed Surveillance does not include entry on, or interference with, property or with wireless telegraphy. Local Authorities **must not** engage in these activities.

2.5 **Intrusive surveillance,** which **cannot** be carried out by Local Authorities, is defined as covert surveillance that:-

- Is carried out in relation to anything taking place on any residential premises or in any private vehicle or place for legal consultation; and

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

2.6 **Covert surveillance** is defined in Section 26(9)(a) of the 2000 Act as any surveillance which is carried out in a manner calculated to ensure that the persons subject to the surveillance are unaware that it is, or may be, taking place.

2.7 A **Covert Human Intelligence Source (CHIS)** is defined in Section 26(8) of the 2000 Act. A person is a human intelligence source if he/she establishes or maintains a personal or other relationship with a person for the covert purpose of facilitating the relationship to obtain information or provide access to any information to another person **or** covertly discloses information obtained by the use of such a relationship, or as a result of its existence. (A CHIS can include inducing, asking or assisting a person to engage in the conduct of a source or obtaining information by using that source. A purpose is covert only if it is conducted in a way calculated to ensure that one party is unaware of the purpose.)

2.8 **Managing the CHIS**

Provision is made in Section 29 of the Act for a CHIS to be carefully managed. This aspect is dealt with in Section 3 (General Rules on Authorisations) and further information is available at Appendix 4. Officers should also note Section 1.5 that the Council will not use Covert Human Intelligence Sources unless there are exceptional circumstances and then only with the approvals set out in this policy.

2.9 **Private information** is defined in Section 26(10) of the 2000 Act as including any information relating to a person's private or family life. This should be broadly interpreted to include an individual's private or personal relationship with others. Family life should be treated as extending beyond the formal relationships created by marriage, civil partnership and private life includes aspects of business and professional life.

2.10 Applications to enter on or interfere with property or with wireless telegraphy **cannot** be made by Local Authorities at the present time.

2.11 **Confidential Information** covers matters which are subject to legal privilege, confidential personal information or confidential journalistic material (see Section 4.8).

2.12 **Collateral Intrusion** – before authorising surveillance, the Authorising Officer must 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. Measures should be taken, wherever practicable, to avoid or minimise unnecessary intrusion into the lives of those not directly connected with the investigation or operation.

2.13 This Code does not generally apply to the use of overt "town centre" or similar police, local authority or private CCTV systems installed for the purpose of prevention or detection of crime and disorder in public places. Members of the public are aware that such systems are in use, for their own protection, and to prevent crime. There may, however, be occasions when the Authority uses overt CCTV for the purposes of a specific investigation or operation. In such cases, authorisation for Directed Surveillance may be necessary.

2.14 In cases where the South Yorkshire Police wish to use the Council's CCTV equipment for Directed Surveillance, the Council's agents should ensure that the Police have obtained an appropriate authorisation and that the documentation agreed under the CCTV protocol, between South Yorkshire Police and the Council, has been completed and retained.

2.15 There is a separate code of practice for the use of CCTV cameras which can be found at:
https://assets.publishing.service.gov.uk/media/619b7b50e90e07044a559c9b/Surveillance_Camera_CoP_Accessible_PDF.pdf

3. GENERAL RULES ON AUTHORISATIONS

3.1 The legislation defines the appropriate persons to give authorisations for Directed Surveillance as Director, Head of Service, Service Manager or equivalent. It also provides for authorisations to be given by more senior officers. For the purposes of the Sheffield City Council this means that the lowest level for an Authorising Officer is that of Service Manager. Officers of the appropriate rank have been appointed by the Council and a list of these can be found at Appendix 5.

3.2 An Authorising Officer will first satisfy him/herself that the authorisation is **necessary** and that the surveillance is **proportionate to what it seeks to achieve**. In assessing whether or not the proposed surveillance is proportionate, the Authorising Officer should balance the intrusiveness of the activity on the target and others who might be affected by it against the need for the activity in operational terms. The activity will not be proportionate if it is excessive in the circumstances of the case or if the information which is sought could reasonably be obtained by other less intrusive means.

3.3 Before authorising surveillance, the Authorising Officer shall also take into account the risk of intrusion into the privacy of persons other than the specified subject of the surveillance (collateral intrusion).

3.4 An application for an authorisation should include an assessment of the risk of any collateral intrusion. The Authorising Officer should take this into account when considering the proportionality of the surveillance. In addition, those carrying out the surveillance **must** inform the Authorising Officer if the investigation or operation unexpectedly interferes with the privacy of individuals who are not covered by the authorisation.

3.5 In cases where the original authorisation may not be sufficient, consideration must be given to whether the authorisation needs to be amended and reauthorised or if a new authorisation is required.

3.6 Authorising Officers should also be aware of any particular sensitivities in the local community where the surveillance is taking place and of similar activities that might be taking place by other public authorities which could impact on the deployment of surveillance. Where surveillance by other authorities may be taking place, contact should be made with the South Yorkshire Police.

3.7 The Home Office Code of Practice on Covert Surveillance states that Authorising Officers **should not** be responsible for authorising matters that they are directly involved in. Where this is unavoidable, it should be highlighted in the central record of authorisations and be brought to the attention of the Surveillance Commissioner at the next inspection.

3.8 It is the responsibility of Authorising Officers to ensure that they have sufficient information and justification to authorise an investigation.

3.9 Each Authorising Officer will nominate the appropriate level of officer to be in charge of the investigation.

3.10 Each Authorising Officer will be responsible for the regular review of authorisations granted, for determining how often a review should take place in each case and for organising effective internal systems within the Service to ensure the effective application for authorisations and their grant or refusal, review, renewal and cancellation.

3.11 Each Authorising Officer will be responsible for ensuring that originals of all the above documentation are provided, on a regular and updated basis, to the RIPA Record Keeper.

3.12 In cases where the Council authorises an agency to conduct Directed Surveillance, the Authorising Officer remains responsible for the recording of authorisations as well as for reviews, renewals and cancellations. The Authorising Officer must also ensure that, when an agency is instructed, the agency identifies an appropriate member of its staff who will be responsible for making the application, the conduct of the investigation and the material obtained until it is finally handed over to the Sheffield City Council.

3.13 **Directed Surveillance** authorisations will last for **three months** but should be cancelled as soon as they are no longer required.

3.14 **CHIS** authorisations may only be authorised by the **Chief Executive** or the General Counsel, **Legal Services after taking advice from the SRO** and, following authorisation, one person within the Service is to be responsible for the day to day running of the CHIS. They will have contact with the human intelligence source, give them their tasks and keep confidential records about what they achieve. The Head of Service should oversee the use made of the CHIS. CHIS authorisations where a vulnerable individual or a juvenile are to be used as a source must be authorised by the **Chief Executive** or, in his unavoidable absence, the Chief Operating Officer**.**

3.15 A risk assessment must be carried out in relation to what issues could be facing the security and welfare of a CHIS in relation to what they are to be tasked to do. This should take place before any authorisation is granted and at any renewal, review and cancellation.

3.16 Further information on the Management of Covert Human Intelligence Sources can be found at Appendix 4.

3.17 A CHIS authorisation will last for **12 months,** but a juvenile source is only permitted to last for **one month.**

3.18 S29B of RIPA came into force on 10th August 2021. It is inserted by the CHIS (Criminal Conduct) Act 2021. Special rules exist where the CHIS activities include criminal conduct. Local authorities do not have the power to grant criminal conduct authorisations

4. AUTHORISATION PROCESS

4.1 The **application for authorisation** for Directed Surveillance shall record, in detail:-

- The grounds on which the Directed Surveillance is necessary, together with an explanation of why it is necessary to use covert surveillance in the investigation. In the case of a local authority, an authorisation for Directed Surveillance can only be given for the purpose of preventing or detecting crime where the offence is punishable by a maximum term of at least 6 months' imprisonment or relates to the underage sale of alcohol or tobacco.

- Why the Directed Surveillance is considered to be proportionate to what it seeks to achieve.

- The identities, where known, of those to be the subject of Directed Surveillance (this may include descriptions of physical appearance) and whether it is likely to interfere with any person's rights to privacy by obtaining private information about that person.

- An outline description of the surveillance proposed to be undertaken (this should include, where possible, the location, any vehicles involved, times, methods and officers involved).

- An explanation of the information which it is desired to obtain as a result of the authorisation.

- An assessment of the risk of any potential collateral intrusion or interference affecting any person other than the subject of the Directed Surveillance and why this is considered necessary.

- The Authorising Officer should be informed if the investigation or operation unwittingly interferes with the privacy of individuals who are not the original subjects of the investigation or operation or covered by the authorisation in some other way (consideration should then be given as to whether a separate authorisation is required) and be made aware of particular sensitivities in the local community where the surveillance is taking place and of any similar activities being undertaken by other public authorities which could impact on the surveillance.

- Details of any confidential information that is likely to be obtained as a consequence of the surveillance.

- Details of the Applying Officer and of the Authorising Officer.
- The date and time from which the authorisation comes into effect.

4.1A **Judicial Approval**

4.1A.1 Following authorisation, an application must be made to the Magistrates' Court for an order approving the grant of the authorisation, before surveillance can take effect. The Magistrate will need to see the original authorisation, together with any supporting documentation, and should also be provided with a partially completed judicial application/order form. The Authorising Officer is responsible for ensuring that the application is made to the Magistrates' Court and the Investigating Officer will make the application to the Court. In some cases, the application may be made by a Council legal representative. For advice/assistance on this process please contact Paul Barber in the Council's Legal Department in the first instance. In his absence, one of the legal managers. For clarity, all Authorisations commence from Magistrates' approval.

4.1A.2 The authorisation takes effect on the day on which the Court approval is granted.

4.2 **Duration of authorisations**

4.2.1 A written authorisation granted by an Authorising Officer for directed surveillance, and approved by the Magistrates' Court, shall cease to have effect (unless renewed) at the end of a period of **three months**, beginning with the day on which it took effect from the date of authorisation by the Magistrates.

4.3 **Reviews**

4.3.1 Regular reviews of authorisations must 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 where the surveillance provides access to confidential information.)

4.3.2 The Authorising Officer should review the authorisation at intervals of no longer than **one month.**

4.4 **Renewals**

4.4.1 If at any time before an authorisation would cease to have effect, the Authorising Officer agrees it is necessary for the authorisation to continue for the purpose for which it was given, he/she may renew the authorisation in writing for a further period of **three months**, beginning with the day when the authorisation would have expired but for the renewal. Each application to renew should be made at least **7 days** before the authorisation is due to expire.

4.4.2 Authorisations may be renewed more than once, provided they continue to meet the criteria for authorisation.

4.4.3 All applications for the renewal of an authorisation for Directed Surveillance should record:-

- Whether this is the first renewal or every occasion on which the authorisation has been renewed previously.
- The information listed at 4.1 above, as it applies at the time of the renewal.
- Any significant changes to the information in the previous authorisation.
- The reasons why it is considered necessary to continue the directed surveillance.
- The content and value to the investigation or operation of the information so far obtained by the surveillance.
- The results of regular reviews of the investigation or operation.
- An estimate of the length of time the surveillance will continue to be necessary.

4.4.4 All applications for the renewal of an authorisation for Directed Surveillance will require the approval of a Magistrate as described in Section 4.1A.1.

4.5 **Cancellations**

4.5.1 The Authorising Officer must cancel an authorisation if he/she becomes satisfied that the surveillance is no longer required or appropriate.

4.5.2 Cancellations must be made using the cancellation form.

4.6 **Ceasing of surveillance activity**

4.6.1 As soon as the decision is taken that Directed Surveillance should be discontinued, the instruction must be given to those involved to stop all surveillance of the subject.

4.6.2 The date and time when such an instruction was given should be recorded in the central record of authorisations and the notification of cancellation.

4.7 **Recording of telephone conversations**

4.7.1 The use of a surveillance device as part of a directed surveillance authorisation should not be ruled out simply because it may incidentally pick up one or both ends of a telephone conversation,

and any such product can be treated as having been lawfully obtained. However, its use would not be appropriate where the sole purpose was to overhear speech which, at the time of monitoring, is being transmitted by a telecommunications system. It must also not involve any modification of, or interference with, the telecommunication system or its operation. Further guidance appears at 3.9 of the Covert Surveillance and Property Interference Code of Practice 2018.

4.8 **Social Media**

Social media is becoming an increasingly important source of information. Reference should be made to the Covert Surveillance and Property Interference Code of Practice 2018 at page 18, 3.10 following.

Although most social media sites allow public access, the Code of Practice suggests that prolonged and systematic surveillance of a particular individual on a site would amount to directed surveillance and a RIPA authority should be obtained. The Code sets out this checklist of questions:-

- Whether the investigation or research is directed towards an individual or organisation;
- Whether it is likely to result in obtaining private information about a person or group of people (taking account of the guidance at paragraph 3.6 above);
- Whether it is likely to involve visiting internet sites to build up an intelligence picture or profile;
- Whether the information obtained will be recorded and retained;
- Whether the information is likely to provide an observer with a pattern of lifestyle;
- Whether the information is being combined with other sources of information or intelligence, which amounts to information relating to a person's private life;
- Whether the investigation or research is part of an ongoing piece of work involving repeated viewing of the subject(s);
- Whether it is likely to involve identifying and recording information about third parties, such as friends and family members of the subject of interest, or information posted by third parties, that may include private information and therefore constitute collateral intrusion into the privacy of these third parties

The Council has issued advice on mitigating the risk of surveillance via viewing social media arising on the intranet at Surveillance and investigation (sheffield.gov.uk) as follows

- "*let customers know if you visit their social media*
- *have a valid work reason for any visit (ie avoid visiting customers' accounts just to see what they are up to)*
- *document that reason and keep a 'screen shot' record of what you look at in your case files*
- *don't use SCC social media accounts to 'friend' customers (to avoid the Council interacting with them on their personal timelines)*
- *always protect your colleagues', customers' and your own privacy and safety by being careful in how you refer to your work or the Council when using your personal social media accounts"*

This page also links to eLearning and the Council's Social networking Policy.

4.9 **Applications that fall outside RIPA**

4.9.1. RIPA authorities are only available where the local authority are involved in preventing or detecting crime or preventing disorder. They are not therefore available where if wish to use covert surveillance in the pursuit of civil matters such as employment issues or civil claims. You can however still pursue covert surveillance because the Investigatory Powers Tribunal case of C v the Police (2006) states that RIPA authorities are only required where a local authority is pursing their core activities rather than general activities that might effect anybody. A local authority as a public body is however subject to Article 8 of the Human Rights Act, the right to respect for private life, which states:-

Article 8 – Right to respect for private and family life

'Everyone has the right to respect for his private and family life, his home and his correspondence.

There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.'

4.9.2 Where it is wished to pursue covert surveillance that falls outside RIPA, the authorisation process set out at 4.1 above should be followed save for obtaining Judicial authority and using the same forms save that the non RIPA nature of the operation must be identified. The authorising officer should record their decision in writing, and it should be retained in accordance with the provisions for document retention in this policy. It should be subject to the same periodic reviews. It is not, as stated, possible to obtain judicial approval for authorisations that fall outside RIPA.

4.9.3 In addition to the above process, any proposal for surveillance which falls outside of RIPA **must** take legal advice from the Council's Legal Services Department and also the SRO at an early stage and throughout the proposal. The advice and/or opinion of the SRO should be recorded in the relevant forms if the operation progresses.

4.8 Special Rules on Authorisations

4.8.1 The 2000 Act does not provide any special protection for "confidential information". However, care must be taken in cases where the subject of the investigation or operation might reasonably expect a high degree of privacy, or where confidential information is involved. (Confidential information relates to matters which are subject to legal privilege, confidential personal information or confidential journalistic material. This includes confidential exchanges between an individual and their priest, MP or doctor).

4.8.2 In cases where, through the use of surveillance, it is likely that knowledge of **confidential information** will be acquired, the use of surveillance **must be** authorised by the **Chief Executive**, or, in his unavoidable absence, the **Executive Director, Resources (SRO).**

4.8.3 The 2000 Act does not provide any special protection for **legally privileged information**. Nevertheless, such information is particularly sensitive and an application for surveillance which is likely to result in the acquisition of legally privileged information must only be made in exceptional and compelling circumstances. Full regard must be had to the particular proportionality issues such surveillance raises. In addition to the reasons why it is considered necessary for the surveillance to take place, the application must include an assessment of how likely it is that information subject to legal privilege will be acquired and whether the purpose (or one of the purposes) of the surveillance is to obtain legally privileged information. Regular reporting may be necessary where privileged information may be gathered so as to be able to decide whether the authorisation should continue. In those cases where legally privileged information has been acquired and retained, it should be reported to the Commissioner or Inspector during his/her inspection and the material made available to him/her if requested.

4.8.4 Similar consideration must also be given to authorisations that involve **confidential personal information** and **confidential journalistic material.** In these cases where such information or material has been acquired and retained, the matter should be reported to the Commissioner or Inspector during his/her next inspection and the material made available if requested. (Confidential personal information is information held in confidence relating to the physical, mental health, or spiritual counselling concerning an individual (whether living or dead) who can be identified from it. Confidential journalistic material includes material acquired or created for the purposes of journalism and held subject to an undertaking to hold it in confidence.)

4.8.5 **CHIS authorisations** may only be authorised by the **Chief Executive** or the General Counsel, Legal Services**.** (see Section 3.15).

4.8.6 In addition, when authorising the conduct or use of a CHIS the Authorising Officer must:-

- Be satisfied that the conduct and/or use of the CHIS is proportionate to what is sought to be achieved.
- Be satisfied that appropriate arrangements are in place for the management and oversight of the CHIS.
- Consider the likely degree of intrusion of all those potentially affected.
- Consider any adverse impact on community confidence that may result from the use or conduct or the information obtained.
- Ensure records contain statutory particulars and are not available except on a need to know basis.

4.8.7 All CHIS authorisations and renewals will require the approval of a Magistrate as described in Section 4.1A.1. and note that CHIS authorisations are not available to Local Authorities for criminal conduct

4.9 **Registration**

4.9.1 The originals of all authorisations, reviews, renewals, cancellations and Court approvals **must** be promptly submitted to the RIPA Record Keeper, who will maintain a central register of all cases of Directed Surveillance or CHIS undertaken by the Sheffield City Council. The central register shall be stored securely.

4.9.2 The retention period for the forms which constitute the central register shall be for 5 years**.** This retention period is considered adequate but not excessive for facilitating independent external inspection.

4.9.3 The officer in charge of investigations shall make arrangements to securely maintain all authorisations, reviews, renewals and cancellations.

5. CENTRAL RECORD OF ALL AUTHORISATIONS

5.1 A centrally retrievable record of all authorisations will be held by the Senior Information Management Officer. Records will be regularly updated whenever an authorisation's documentation (granted, reviewed, renewed or cancelled) is completed and passed from the Authorising Officer to the Information and Knowledge management Team. The record will be made available to the relevant Commissioner

or an Inspector from the Office of Surveillance Commissioners upon request. These records will be retained for a period of five years from the ending of the authorisation and will contain the following information:-

- The type of authorisation.
- The date the authorisation was given.
- The name and grade of the Authorising Officer.
- The unique reference number (URN) of the investigation or operation.
- The title of the investigation or operation (if any), including a brief description and the name of subjects, if known.
- If the authorisation is renewed, when it was renewed and who authorised the renewal, including the name and rank/grade of the Authorising Officer.
- Whether the investigation or operation is likely to result in obtaining confidential information as defined in this Code of Practice.
- The date the authorisation was cancelled.

5.2 In all cases, the City Council must maintain the following documentation (which need not form part of the centrally retrievable record):-

- 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.
- A record of the period over which the surveillance has taken place.
- The frequency of reviews prescribed by the Authorising Officer.
- A copy of any renewal of an authorisation, together with the supporting documentation submitted when the renewal was requested.
- The date and time when any instruction was given by the Authorising Officer.

Officers need to ensure that the Records Keeper is made aware of the dates of Authorisations, Reviews, Approvals and Cancellations in order to keep the records up to date. Copies of the documents are also required after the end of the vent (i.e. once completed and cancelled).

5.3 **Retention and Destruction of the Product**

5.3.1 Where the product of surveillance could be relevant to pending or future criminal or civil proceedings, it should be retained in accordance with established disclosure requirements for a suitable further period, commensurate to any subsequent review.

5.3.2 Particular attention is drawn to the requirements of the Code of Practice issued under the Criminal Procedure and Investigations Act 1996. This requires that material which is obtained in the course of a criminal investigation and which may be relevant to the investigation must be recorded and retained.

5.3.3 There is nothing in the 2000 Act which prevents material obtained from properly authorised surveillance from being used in other investigations. The Council must ensure that arrangements are in place for the proper handling, storage and destruction of material obtained through the use of covert surveillance

5.3.4 Authorising Officers must ensure compliance with the appropriate Data Protection requirements and any relevant Codes of Practice produced by individual authorities relating to the handling and storage of material.

5.4 Dissemination, copying and retention of material obtained through authorised surveillance

5.4.1 Dissemination, copying and retention of material obtained through the authorized surveillance must be limited to the minimum necessary for authorised purposes. Something is necessary for the authorised purposes if the material:

- is, or is likely to become, necessary for any of the statutory purposes set out in legislation in relation to covert surveillance including RIPA
- is necessary for facilitating the carrying out of the functions of public authorities under those Acts;
- is necessary for facilitating the carrying out of any functions of the Commissioner or the Investigatory Powers Tribunal;
- is necessary for the purposes of legal proceedings; or
- is necessary for the performance of the functions of any person by or under any enactment

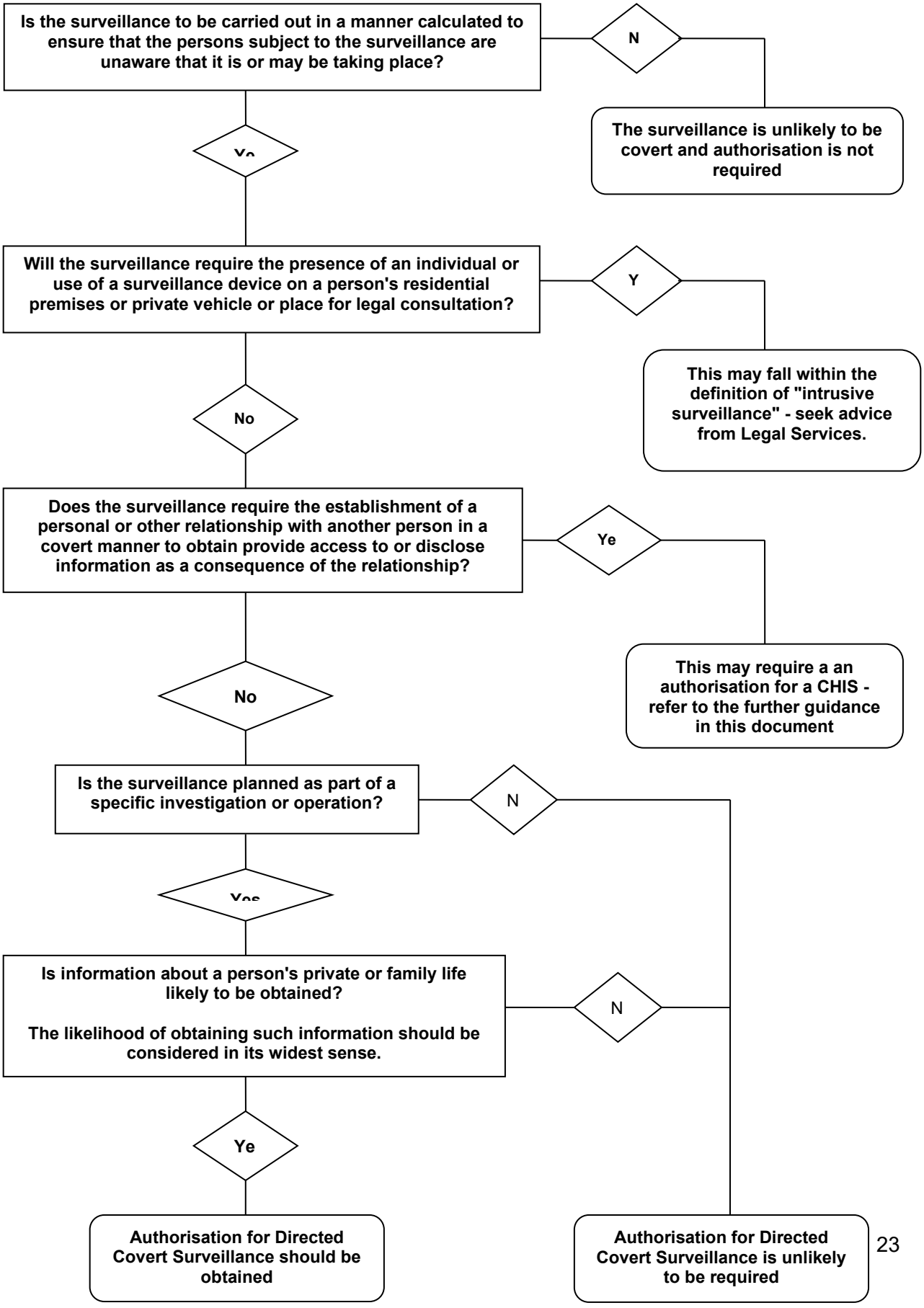
5.4.2 All data obtained under RIPA should be clearly labelled and stored in accordance with the Council's retention policy.

5.4.3 Material obtained from surveillance should only be retained so long as is necessary for the authorised purpose. It should be subject to periodic review. All persons to whom the information is disseminated should be made aware of this principle and reviews should be carried out to make sure that they have not retained the information longer than is necessary.

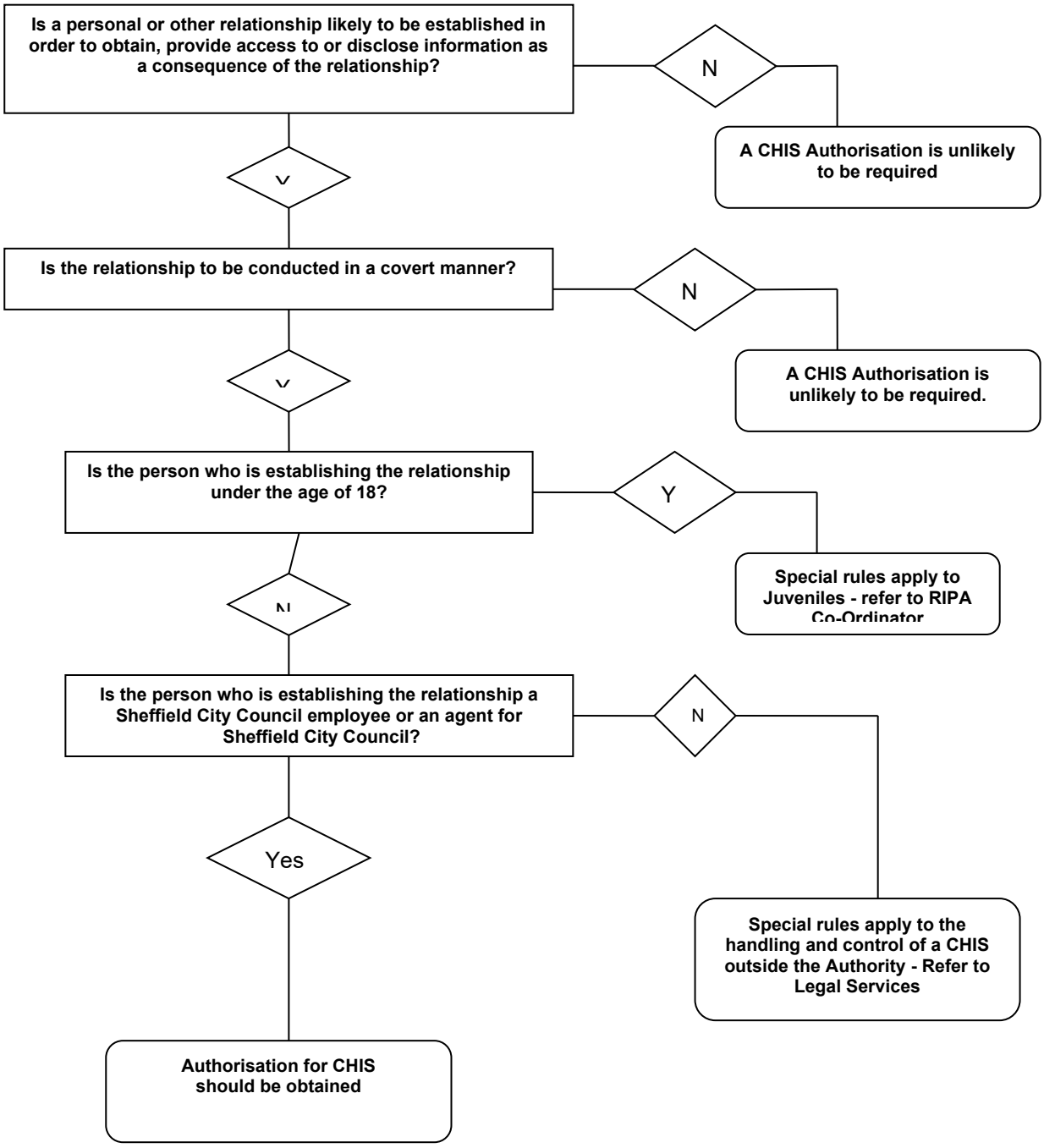
5.4.4 Particular care should be taken in the storage and destruction of confidential or privileged material such as journalistic material, material subject to legal professional privilege or confidential personal information.

APPENDIX 1

Determination of Whether DCS Authorisation is Required



Determination of Whether CHIS Authorisation is Required



APPENDIX 2

Authorising Officers duties:

Duty	Para
Only grant an authorisation for directed surveillance if s/he believes that it is necessary for the purpose of preventing or detecting crime and that the offence is punishable by a maximum term of at least 6 months' imprisonment or relates to the underage sale of alcohol or tobacco, AND	1.2
Only grant an authorisation that it is proportionate to what is sought to be achieved by carrying out surveillance.	3.2
Before authorising surveillance, take into account the risk of collateral intrusion.	3.3
Before authorising surveillance, take into account (whilst considering proportionality), an assessment of the risk of any collateral intrusion.	3.4
Be aware of particular sensitivities in the local community where the surveillance is taking place and of similar activities that might be taking place by other public authorities.	3.6
Unless it is unavoidable, not issue authorisations for investigations in which s/he are directly involved.	3.7
Acknowledge that responsibility for authorising the carrying out of Directed Surveillance rests with them.	3.8
Ensure that they have sufficient information and justification to authorise an investigation.	3.8
Regularly review authorisations granted, to assess the need for the surveillance to continue.	3.10
Determine how often a review should take place in each case.	3.10
Renew authorisations where appropriate	3.10
Make sure that the central record of all authorisations is regularly updated whenever an authorisation is granted, reviewed, renewed or cancelled.	3.11 4.9.1
Continue to be responsible for authorisations, reviews, renewals and cancellations in cases where agencies are used.	3.12

Duty	Para

Ensure that any agency used identifies an appropriate member of its staff to be responsible for making the application, the conduct of the investigation and material obtained.	3.12
Ensure that an application is made to the Magistrates' Court for approval of the authorisation.	4.1A.1
Cancel the authorisation if s/he is satisfied that the Directed Surveillance no longer meets the criteria upon which it was authorised.	4.5.1
On cancellation, issue appropriate instructions to officers in charge of investigations.	4.6.1
Take particular care before authorising surveillance where the subject of the investigation might reasonably expect a high degree of privacy, or where confidential information is involved.	4.8.1
Make sure that authorisation is by the Chief Executive, or in his unavoidable absence, the Executive Director, Resources, in cases where confidential information is likely to be acquired.	4.8.2
Take into account (whilst considering proportionality) any assessment of how likely it is that information subject to legal privilege will be acquired.	4.8.3
Require regular reporting (if necessary) where legally privileged information may be gathered so as to be able to decide whether the authorisation should continue.	4.8.3
Give similar consideration to authorisations that involve confidential personal information and confidential journalistic material as to those involving legally privileged information.	4.8.4
Take into account additional matters when authorising a CHIS.	4.8.6
Ensure compliance with the appropriate data protection requirements.	5.3.4

APPENDIX 3

Officers in charge of investigations - duties:

Duty	Para
Seek authorisation for surveillance where it is likely to interfere with any person's rights to privacy by obtaining private information about that person.	4.1
Make proper applications for authorisation for Directed Surveillance.	4.1
Record appropriate detail where the authorisation relates to an urgent case.	4.1
Inform the Authorising Officer if the investigation unexpectedly interferes with the privacy of individuals who are not covered by the authorisation.	4.1
Make the Authorising Officer aware of particular sensitivities in the local community where the surveillance is taking place and of similar activities being undertaken by other public authorities which could impact on the surveillance.	4.1
Make the application to the Magistrates' Court for approval of the authorisation.	4.1A.1
Ensure that authorisations are regularly reviewed.	4.3.1
Apply for renewal shortly before the expiry of the authorisation period.	4.4
Cancel the authorisation when the surveillance is completed.	4.5.2
Act immediately to terminate surveillance when instructed by the Authorising Officer.	4.6
Take particular care where the subject of the investigation might reasonably expect a high degree of privacy, or where confidential information is involved.	4.8.1
Only apply for authorisation in exceptional and compelling circumstances where the acquisition of legally privileged information is likely to result.	4.8.3
Include an assessment of how likely it is that information subject to legal privilege will be acquired in an application for authorisation.	4.8.3
Obtain advice from a City Council legal adviser where there is any doubt about the handling, etc of information which may be subject to legal privilege.	4.8.3
Give similar consideration to applications for authorisation that involve confidential personal information and confidential journalistic material as to those involving legally privileged information.	4.8.4
Maintain the appropriate documentation.	4.9.3
Properly store and retain the product of surveillance.	5.3

APPENDIX 4

MANAGEMENT OF COVERT HUMAN INTELLIGENCE SOURCES

(Information Note: The use of a CHIS in Council investigations is most unlikely. Any officer contemplating such use should immediately seek advice from the Director of Legal and Governance.)

Additional Notes on CHIS (This is an extract from the Home Office Code of Practice on CHIS)

MANAGEMENT OF SOURCES

Tasking

1. Tasking is the assignment given to the source by the persons defined at sections 29(5)(a) and (b) of the 2000 Act, asking him to obtain information, to provide access to information or to otherwise act, incidentally, for the benefit of the relevant public authority. Authorisation for the use or conduct of a source is required prior to any tasking where such tasking requires the source to establish or maintain a personal or other relationship for a covert purpose.

2. The person referred to in section 29(5)(a) of the 2000 Act will have day to day responsibility for:

   - dealing with the source on behalf of the authority concerned;

   - directing the day to day activities of the source;

   - recording the information supplied by the source; and

   - monitoring the source's security and welfare;

3. The person referred to in section 29(5)(b) of the 2000 Act will be responsible for the general oversight of the use of the source.

4. In some instances, the tasking given to a person will not require the source to establish a personal or other relationship for a covert purpose. For example a source may be tasked with finding out purely factual information about the layout of commercial premises. Alternatively, a Trading Standards Officer may be involved in the test purchase of items which have been labelled misleadingly or are unfit for consumption. In such cases, it is for the relevant public authority to determine where, and in what circumstances, such activity may require authorisation.

5. It is not the intention that authorisations be drawn so narrowly that a separate authorisation is required each time the source is tasked. Rather, an authorisation might cover, in broad terms, the nature of the source's task. If this changes, then a new authorisation may need to be sought.

6. It is difficult to predict exactly what might occur each time a meeting with a source takes place, or the source meets the subject of an investigation. There may be occasions when unforeseen action or undertakings occur. When this happens, the occurrence must be recorded as soon as practicable after the event and, if the existing authorisation is insufficient it should either be updated and re-authorised (for minor amendments only) or it should be cancelled and a new authorisation should be obtained before any further such action is carried out.

7. Similarly where it is intended to task a source in a new way or significantly greater way than previously identified, the persons defined at section 29(5)(a) or (b) of the 2000 Act must refer the proposed tasking to the authorising officer, who should consider whether a separate authorisation is required. This should be done in advance of any tasking and the details of such referrals must be recorded.

Management responsibility

8. Public authorities should ensure that arrangements are in place for the proper oversight and management of sources, including appointing individual officers as defined in section 29(5)(a) and (b) of the 2000 Act for each source.

9. The person responsible for the day-to-day contact between the public authority and the source will usually be of a rank or position below that of the authorising officer.

10. In cases where the authorisation is for the use or conduct of a source whose activities benefit more than a single public authority, responsibilities for the management and oversight of that source may be taken up by one authority or can be split between the authorities.

Security and welfare

11. Any public authority deploying a source should take into account the safety and welfare of that source, when carrying out actions in relation to an authorisation or tasking, and to foreseeable consequences to others of that tasking. Before authorising the use or conduct of a source, the authorising officer should ensure that a risk assessment is carried out to determine the risk 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 cancellation of the authorisation, should also be considered at the outset.

12. The person defined at section 29(5)(a) of the 2000 Act is responsible for bringing to the attention of the person defined at section 29(5)(b) of the 2000 Act any concerns about the personal circumstances of the source, insofar as they might affect:

- the validity of the risk assessment
- the conduct of the source, and
- the safety and welfare of the source.

13. Where deemed appropriate, concerns about such matters must be considered by the authorising officer, and a decision taken on whether or not to allow the authorisation to continue. CHIS authorities are not available for criminal conduct.

APPENDIX 5

SHEFFIELD CITY COUNCIL

REGULATION OF INVESTIGATORY POWERS ACT 2000

AUTHORISING OFFICERS

Kate Josephs – Chief Executive

Resources Team

Claire Taylor – Chief Operating Officer (Senior Responsible Officer)
David Hollis – General Counsel

Neighbourhood Services

Ian Ashmore – Head of Environmental Regulation