WEST WILTSHIRE DISTRICT COUNCIL

REGULATION OF INVESTIGATORY POWERS ACT 2000 (RIPA)

SURVEILLANCE PROCEDURE

Introduction

1.0 This procedure details the ways in which covert surveillance should be authorised, conducted and recorded.

1.1 Surveillance is regulated by the Regulation of Investigatory Powers Act 2000 (RIPA).

1.2 The Government has appointed Surveillance Commissioners to administer the legislation and, as a Local Authority, we can be audited on our performance of surveillance at any time.

1.3 The Act provides specific definitions for the various types of surveillance (covert, directed and intrusive and are described in section 1.9 to 1.13 below) and prescribes the authorisation and conduct of each.

1.4 Any directed surveillance work must be authorised to have the legal protection of RIPA from potential Human Rights Act (Article 8) breaches.

1.5 **Surveillance which is not properly authorised may be unlawful and result in costs being awarded against the Council. Officers and all external agencies employed by West Wiltshire DC must comply with RIPA and this procedure. Failure to comply with this procedure may result in disciplinary action in line with the Council's policy**.

1.6 The law makes no distinction between investigation of a complaint by the Council, (for example, of alleged statutory nuisance) and the type of surveillance carried out by the police, customs or security services.

1.7 Each investigation that includes an element of directed surveillance will require an authorisation.

1.8 The authorisation procedure covers both directed surveillance and **C**overt **H**uman **I**ntelligence **S**ources (CHIS), and contains the relevant forms for both.

Definitions

1.9 **Covert Human Intelligence Sources (CHIS)**

A person who establishes or maintains a personal or other relationship with a person for the purpose of facilitating the doing of anything that

- covertly uses such a relationship to obtain information or to provide access to information to another person; or
- covertly discloses information obtained by the use of such a relationship, or as a consequence of the existence of such a relationship.

1.10 **Covert**

Surveillance is covert if, and only if, it is carried out in a manner that is calculated to ensure that persons who are subject to the surveillance are unaware that it is or may be taking place.

1.11 **Private Information**

Private Information in relation to a person includes any information relating to his/her private and family life, home or correspondence.

This includes:

- details of relationships
- details of one's home that are not open to public view
- details of business or work life

The fact that something takes place in public does not mean that it is not part of someone's private life.

1.12 **Directed surveillance**

This is surveillance which is covert but not intrusive and is undertaken:

i) for a specific investigation

ii) to obtain private information, and

iii) is a planned activity, (i.e. not reactive)

1.13 **Intrusive surveillance**

Intrusive surveillance includes planned covert surveillance:

i) of anything taking place in any **residential** premises or in any private vehicle; ***and***

ii) involves the presence of an individual in the premises or vehicle ***or*** is carried out by means of a surveillance device in the premises or vehicle, or which can monitor as well as if it were in the premises or vehicle.

Types of Surveillance

2.0 Examples of **directed surveillance** include the planned:

- observation of a building to monitor criminal activity
- use of CCTV to monitor a known hot spot for public disorder or fly tipping.

2.1 **Intrusive surveillance**. Local authorities are not permitted to carry out intrusive surveillance

2.2 The Council rarely uses CHIS so if you are considering this seek further legal advice. More information is given in section 13 of this procedure.

Authorisations

3.0 Planned covert surveillance activities must be authorised, in writing, by an **authorising officer** prior to taking place.

3.1 Surveillance may only be authorised for the purpose of:

- Preventing or detecting crime or of preventing disorder

3.2 A written authorisation would not be needed in the following:

(a) in case of an immediate reaction to events requiring directed surveillance, where it would not be reasonably practical to obtain authorisation.

Even in these circumstances, officers should attempt to obtain authorisation by telephone where possible.

(b) Where the person being investigated has been notified of the fact, (including the type of monitoring to be used and the timescale for the monitoring). For example, where a warning letter has been sent to the person responsible notifying them that their activities may be monitored, or a warning sign is displayed. In this case the surveillance would not be covert.

(c) Authorisations can be given orally, if waiting for the authorising officer to give consent in writing would be likely to endanger life or jeopardise the investigation.

An authorisation is not deemed urgent if the need for an authorisation has been neglected, or the delay is of the authorising officers own making.

If an authorisation is given orally, then it should be confirmed, in writing, as soon as possible.

NB: The granting of authorisations in the above circumstances is extremely unlikely in a local authority setting, and seek legal advice before obtaining authorisations in these circumstances.

3.3 Where doubt exists as to whether a given activity is covered by RIPA or not, an authorisation should be sought to obtain the potential benefits that an authorisation would confer.

3.4 Where time permits (and this should include all planned surveillance), authorisation should be obtained from the relevant Service Manager (listed below).

3.5 The service managers permitted to authorise surveillance requests (**authorising officer**) are:

- Environmental Health Service Manager
- Revenues and Benefits Service Manager
- Development Control Service Manager
- Head of Legal and Democratic Services
- Head of Human Resources & Customer Services

3.6 RIPA authorisations are only for specific investigations and must be actively renewed or cancelled once the specific surveillance is complete.

Flowchart

4.0 In all cases where surveillance is undertaken, the steps described in the flowchart in Appendix 1 must be followed. Explanatory Notes for specified parts of that flowchart are in Appendix 2 to this procedure.

Application/Authorisation Form

5.0 There are four forms for directed surveillance. These cover authorisation, review, renewal and cancellation of surveillance. These forms must be completed by the **investigating officer** when it is appropriate to do so.

5.1 The authorising officer must consider the impact of surveillance on the privacy of either specified individuals or unknown persons. Each case will therefore be different. As an Authorisation covers the whole of an investigation or operation and lasts for 3 months it is important, when completing an application, that the **investigating officer**:

- gives a detailed description of why the surveillance is necessary and why the required information cannot be gained in any other way;
- a detailed description of why surveillance is proportionate, including the steps to be taken to minimise collateral intrusion/risk of gathering confidential information; and
- describes in detail the activities to be undertaken so that it is clear exactly what is being authorised

5.2 Completion of the first section of the form is the responsibility of the officer tasked to conduct the surveillance (**investigating officer**).

5.3 The form must then pass to the **authorising officer**. The **authorising officer** must explain why they believe the surveillance or CHIS is necessary and proportionate and if not authorised, explain their reasons for refusal on the form.

Benefits of authorisation

6.0 A RIPA authorisation guarantees that covert directed surveillance/CHIS is lawful for all purposes. It also ensures that we respect the rights of our residents to privacy under the Human Rights Act. Therefore, it is vital that officers carry out surveillance strictly in accordance with the activities described in the authorisation so that:

- they know their actions are lawful; and
- the Council is safe from legal action.

This reinforces the need for a clear and detailed statement in the application for authorisation of the activities to be undertaken.

Recording and filing authorisations

7.0 The authorising officer must ensure that the authorisation documents are centrally recorded. Any officer who authorises surveillance must forward the documents to the Environmental Health Service Manager as soon as is reasonably practicable.

7.1 The Environmental Health Service Manager will keep a register of all authorisation documents (known as the **authorisation register**). All applications must be allocated a unique reference number.

7.2 The Head of Legal and Democratic Services will undertake a monitoring role, and will periodically review the authorisation register and index to ensure compliance with the legislation and procedures, and to check that authorisations, extensions, renewals and cancellations are being granted in appropriate circumstances.

7.3 The RIPA procedures shall be reviewed every two years in co-ordination with the biannual review of the corporate enforcement policy.

Duration of Authorisations and Reviews

8.0 Authorisations last for 3 months, unless cancelled sooner or renewed. Authorisations must be cancelled as soon as the investigation has been completed, and this is to be recorded on the cancellation of directed surveillance authorisation form.

8.1 Authorisations must periodically be reviewed to ensure that the necessary statutory criteria and the reason for the authorisation still applies.

8.2 The review period will be decided by the authorising officer. It should be appropriate to the circumstances of each case and recorded on the review of directed surveillance authorisation form and this must be placed in the authorisation register.

Renewal of authorisations

9.0 If continued surveillance is required, the investigating officer must make arrangements for it to be renewed before the authorisation expires. When considering an application for renewal the authorising officer must:

- be satisfied that the necessary statutory criteria still applies;
- the authorising officer shall examine the information obtained to assess whether there has been excessive collateral intrusion. If so the method of surveillance may have to be altered.

Any renewals must be recorded on the renewal of directed surveillance authorisation form, and this must be placed in the authorisation register.

Cancellation of authorisations

10.0 All authorisations must be cancelled as soon as the surveillance has been completed.

10.1 The authorising officer must complete the cancellation of directed surveillance authorisation form and this must be placed in the authorisation register.

Collateral intrusion

11.0 Collateral intrusion is the often unavoidable intrusion into the privacy of people who are not the subject of the surveillance. For example, if you are observing a house in the middle of a terrace it is very likely that you will be able to see the adjoining properties on either side.

11.1 Before seeking an authorisation the investigating officer should consider how to minimise the risk of collateral intrusion. The authorising officer should satisfy him/herself that all reasonable steps have been taken to minimise the risk. They

may feel that where a large amount of collateral intrusion is likely then the chosen surveillance method may be disproportionate to the importance of the investigation.

11.2 When considering the risk of collateral intrusion the investigating and authorising officer should also consider the particular sensitivities of the local community. For example will the intrusion into privacy be regarded as more severe because of religious or ethnic views.

11.3 Occasionally unexpected events may occur which increase the risk of collateral intrusion. In such cases the investigating officer should discuss with the authorising officer whether the authorisation needs amendment or even a fresh authorisation.

11.4 Once an investigation is complete, information obtained as a result of collateral intrusion must be strictly controlled. It should not be used or disclosed except in accordance with the Data Protection Act 1998 and/or an order of the court.

11.5 Officers should seek legal advice on what use, if any, should be made of this information. It should only be edited with the agreement of both parties to the proceedings or in accordance with an order of the court.

Confidential Information

12.0 Surveillance which is likely to result in the obtaining of information which:-

(i) relates to communications between a minister of religion and an individual about the latter's spiritual welfare;

(ii) is subject to medical or journalistic confidentiality.

(iii) is subject to legal professional privilege.

should only be regarded as proportionate and appropriate for authorisation in exceptional and compelling circumstances.

12.1 Before using any information falling into the above categories, the investigating officer should take legal advice.

12.2 Note - the use of a CHIS is more likely to result in the obtaining of confidential information, any application for an authorisation should clearly state whether the purpose for the use of a CHIS is to obtain confidential information.

12.3 Officers should seek legal advice on what use, if any should be made of this information. It should only be edited with the agreement of both parties to the proceedings or in accordance with an order of the court.

12.4 Where confidential information may be acquired, the CHIS must be authorised by the Chief Executive, or in his absence the Deputy Chief Executive.

Specific Rules for using a CHIS (Covert Human Intelligence Source)

13.0 All of the above procedures apply equally for the use of a CHIS, and there are some additional procedures outlined below that should be applied.

13.1 When using a CHIS they should be reminded not to do anything that is unlawful – do not commit a criminal act.

13.2 The use of a CHIS must be explained on the application form, and why this conduct or use of the source is proportionate to what it seeks to achieve

Use of vulnerable and juvenile sources

13.3 A vulnerable individual is a person who is, or may be, in need of community care services by reason of mental or other disability, age or illness and who is, or may be, unable to take care of himself/herself, or unable to protect himself/herself against significant harm or exploitation. Any individual of this description should only be authorised to act as a source in the most exceptional circumstances.

13.4 A juvenile source is someone under the age of 18 years. On no occasion should the use or conduct of a source under 16 years old be authorised to give information against the parents or any person who has parental responsibility for him/her.

13.5 If you use a CHIS who is under 16, the authorising officer is responsible for ensuring that an appropriate adult is present at any meeting. An appropriate adult means a parent or guardian, person who has assumed responsibility for the wellbeing of the CHIS or in their absence a person responsible who is over 18 who is neither a member of, or employed, by the Council.

13.6 For such applications the Chief Executive must authorise a juvenile CHIS.

13.7 **NB.** In addition a risk assessment must be carried out in accordance with the Regulation of Investigating Powers (Juveniles) Order 2000 SI 2793.

13.8 Authorisation for juveniles only lasts one month.

Management of CHIS sources

14.0 The case officer will be the **source handler** with day to day responsibility for:-

(i) dealing with the source.

(ii) directing the day to day activities of the source.

(iii) recording the information supplied by the source.

(iv) monitoring the sources security and welfare.

14.1 In the case of a CHIS, there should also be a nominated **co-handler**. All meetings with the CHIS should be attended by both the handler and the co-handler.

14.2 The case officer's line manager (**the controller**) will be responsible for the general oversight of the use of the source.

14.3 The source handler (case officer) shall carry out a risk assessment of the activity which the CHIS is being asked to undertake and the likely consequences should the role become known.

14.4 The source handler (case officer) must bring to the attention of the controller (case officer's line manager) any information of the personal circumstances of the source that may affect the conduct of the source or the personal safety of the source. The

controller must decide whether or not to report such information to the authorising officer in terms of whether or not to conduct a review of the Authorisation.

14.5 Specific records must be kept in relation to a CHIS which are detailed in the Regulation of Investigatory Powers (Source Records) Regulations 2000. The relevant details which must be recorded are:-

a) the identity of the source;
b) the identity, where known, used by the source;
c) any relevant instigating authority other than the Authority maintaining the records;
d) the means by which the source is referred to within each relevant investigatory 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 S.29(5)(a) to (c) of the 2000 Act or in any order made by the Secretary of State under S.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.

Closed Circuit Television (CCTV) use

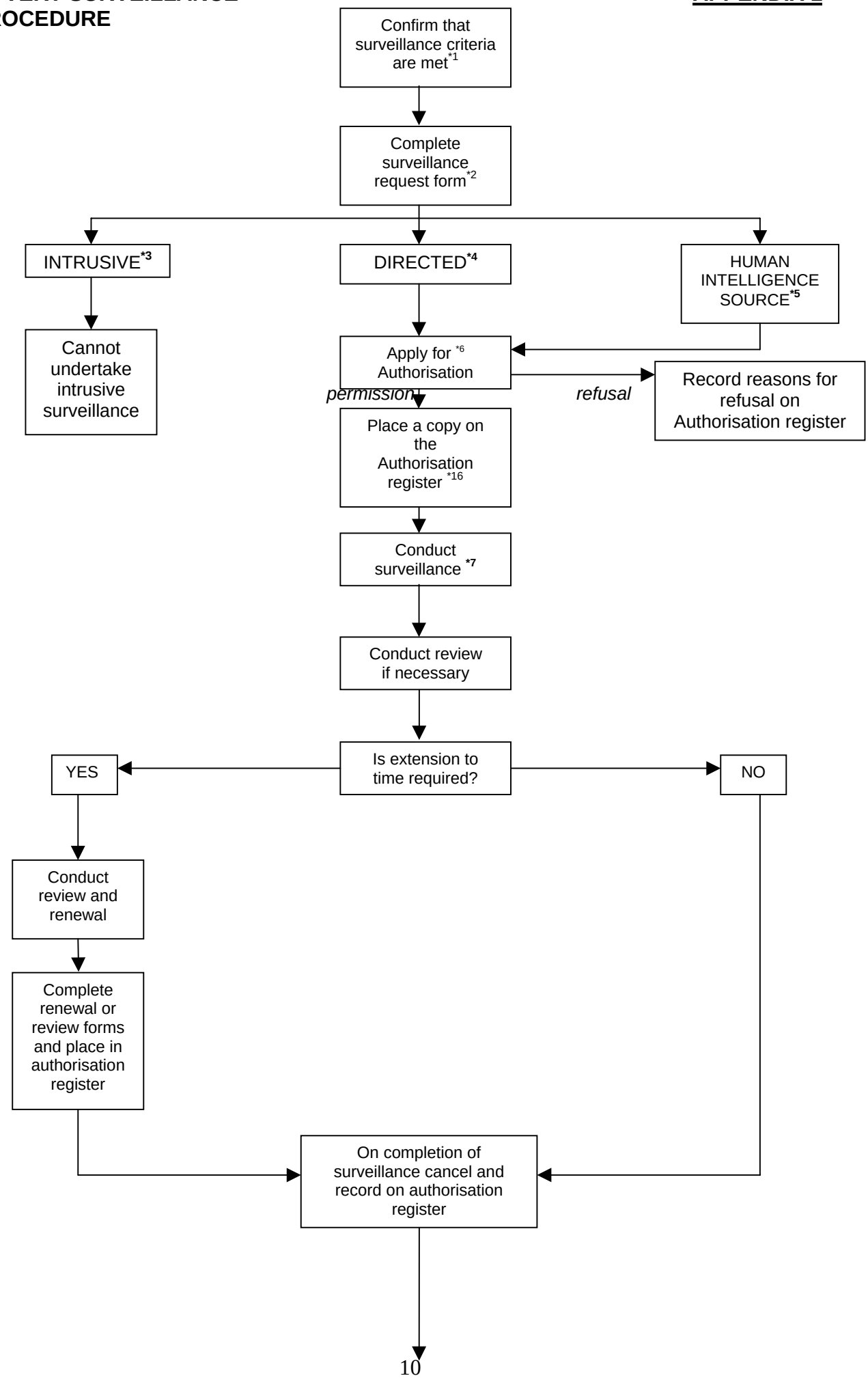
15.0 Whilst the council does not operate CCTV systems in the town centre areas, it does use CCTV equipment at the Bradley Road and Riverway offices and at the Hillside and Kingsbury Square hostels.

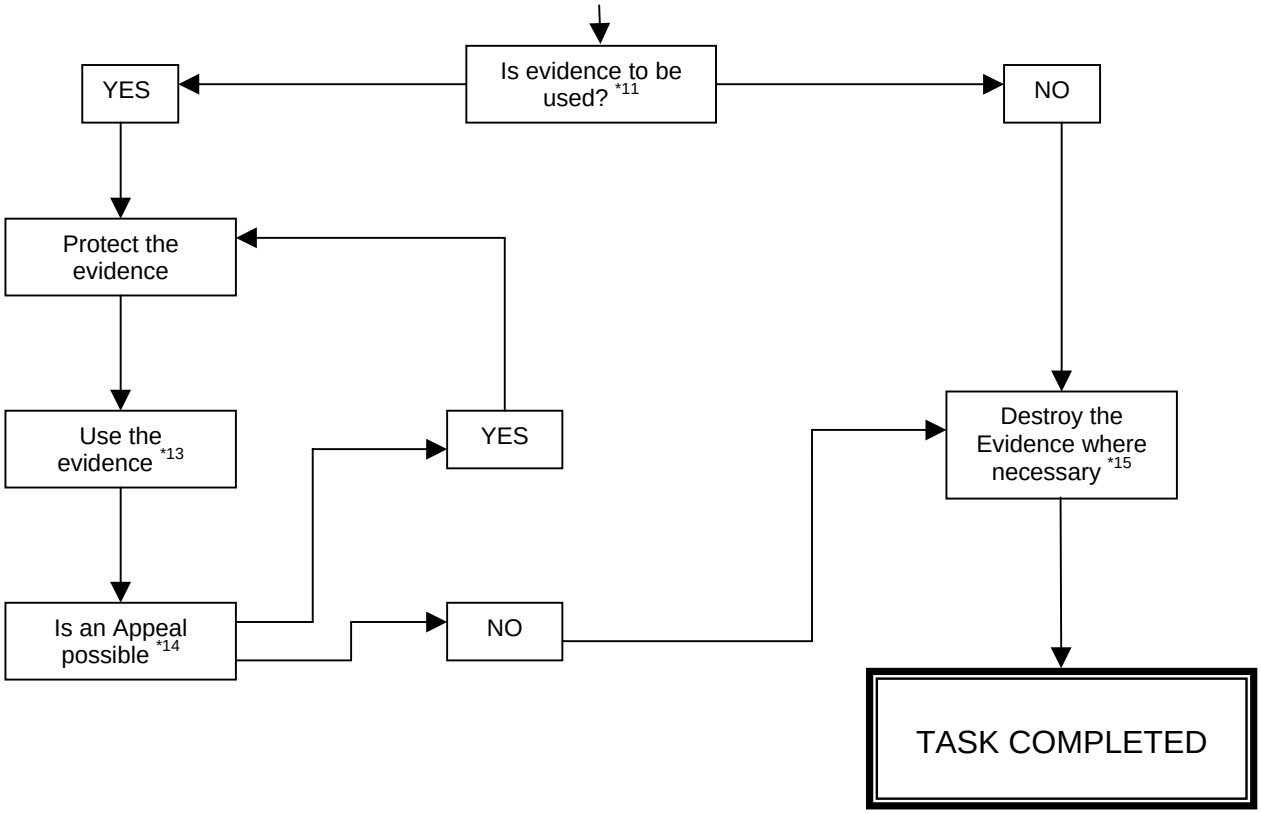
15.1 The presence of CCTV equipment is clearly signed, and its overt use is covered by the code of practice for the operation of CCTV camera equipment issued by the Property and estates service.

15.2 If the equipment were to be used in a proactive, covert way this would require an authorisation as specified in section 5 of this procedure.

COVERT SURVEILLANCE PROCEDURE

APPENDIX 1




Is evidence to be used? *11
YES
NO
Protect the evidence
Use the evidence *13
YES
Is an Appeal possible *14
NO
Destroy the Evidence where necessary *15
TASK COMPLETED

APPENDIX 2

EXPLANATORY NOTES FOR SURVEILLANCE FLOW CHART

The notes which follow correspond to the asterisk numbers attached to certain boxes in the Flowchart at Appendix 1.

Note 1 Before submitting the application for Authorisation, the investigating officer must satisfy himself/herself that the following criteria have been met:

a) The surveillance will be covert (see section 1.10 of the procedure)

b) There are proper grounds for surveillance (see section 3.1 of the procedure)

c) The degree of surveillance will be proportionate to what it is desired to achieve and be the least intrusive method

Note 2 For an initial application for authorisation the investigating officer should complete the first part of the application form.

Notes 3, 4 & 5 Officers must use the relevant application form for either directed surveillance or CHIS.

Note 6 Under normal circumstances, the Authorisation must have been approved by the relevant service manager (authorising officer) before the specified surveillance can take place.

Where time is short a more senior officer may authorise surveillance.

In some cases, surveillance may be conducted without authorisation (see section 3.2 of the procedure).

For juvenile and vulnerable CHIS applications see section 13.3 of the procedure.

Note 7 Surveillance may ***only*** be conducted by the officer(s) named in the Authorisation and ***only*** in strict accordance with any conditions applied to it.

Note 8 Authorising Officers should note that surveillance is authorised for 3 months.

Note 9 Where an extension to time (renewal) of Authorisation is required, application should be made in sufficient time to ensure that it can be authorised.

Note 10 When surveillance has been completed or if it is cancelled before the end of the 3-month period, the investigating case officer is to notify the fact to the authorising officer. The authorising officer will then complete the form, cancellation of a directed surveillance authorisation which must be placed on the authorisation register.

Note 11 On completion of the surveillance operation, a decision should be made as quickly as possible on whether any evidence gathered is to be used.

Note 12 Any evidence to be kept must be properly protected.

Note 13 Before using the evidence, it should be scrutinised with a view to identifying *collateral intrusion* material (see section 11 of the procedure) where possible. If necessary, the advice of Legal Services on whether the evidence should be used (see section 11.5 of the procedure).

Note 14 Following a Court hearing any evidence obtained from surveillance must be preserved, under protected conditions, so long as any possibility of an Appeal remains.

Note 15 If evidence resulting from surveillance is not to be used, or when all possibility of further legal proceedings are ended in the case, such evidence should be destroyed if it contains anything which may be regarded as *collateral intrusion* or confidential information (see section 12 of the procedure).

Photographs should be shredded, digital photographs stored on PC should be deleted, and backups destroyed. Video footage and tape recordings may be either erased or taped over.

Note 16 The Environmental Health Service Manager is responsible for monitoring and maintaining a central authorisation register. Copies of all authorisations, renewals, refusals and cancellations shall be forwarded to the Environmental Health Service Manager as soon as reasonably practicable.