Clackmannanshire Council

REGULATION OF INVESTIGATORY POWERS (SCOTLAND) ACT 2000

Policy for Authorising Covert Surveillance Operations.

Version Tracking			Comments
V2	January 2007	Reported to Council for approval (15 Feb 2007)	(Appendix 1 to report) - RR
V2.1	March 2008	Updated following inspection report, Jan 2008.	
V2.2	May 2010	Updated to show the Council's restructuring	Remove 'Administration & Legal Services' replace with 'Strategy and Customer Services' - RR
V2.2.1	September 2010	General review and update	Reflecting Commissioner's recommendations - RR
V2.3	January 2011	Improvements	Separate guidance on use of forms etc into another document – RR
V2.4	October 2011	Review and update	Take account of experience in other areas
V2.5	July 2012	Up-dated to change reference to Monitoring Officer (in relation to being an authorising officer)	
V2.6	Mar 2013	Up-dated in line with recommendations in Asst Surveillance Commissioner's Report	
V2.7	December 2014	Updated to show new titles for the Council's Directors (Depute Chief Executive and Executive Director)	

The Regulation of Investigatory Powers (Scotland) Act 2000 (RIP(S)A)

Part 1

1. Introduction

Both the Regulation of Investigatory Powers (Scotland) Act 2000 (RIP(S)A) and the Human Rights Act 1998 impact on the way the Council conducts its business. Amongst other things, the Human Rights Act (HRA) entitles citizens to expect that their privacy will be respected in relation to their private life, family life, their home and correspondence. It also entitles them to peaceful enjoyment of their possessions. The Regulation of Investigatory Powers (Scotland) Act recognises that these rights may, nevertheless, be lawfully infringed in some circumstances provided the method used is lawful, has a legitimate aim, the action is necessary, and is proportional to what it would achieve.

2.0 Policy Objective

2.1 The aim of this policy is to provide the framework outlining the Council's process for authorising and managing covert surveillance operations under RIP(S)A, and to set the parameters for expected good practice. Guidance documents supporting the objectives will be made available to all affected staff.

3.0 Scope of the Policy

3.1 This policy applies in all cases where *directed surveillance* is being planned or carried out.

3.2 The policy does not apply to:

I. Observations carried out overtly
II. ad-hoc observations that do not involve systematic surveillance of any specific person.
III. Unplanned observations made as an ***immediate*** response to events where it was not reasonably practicable to seek authorisation
IV. The surveillance of staff for disciplinary investigations or other purposes unless the purpose relates directly to a regulatory function of the Council.

Regardless of the above, wherever there is doubt, and a perceived need to obtain information or evidence in a structured manner, the good practice identified by this policy should be followed.

3.3 The policy framework will be supported by guidance papers which focus on particular technical aspects of managing covert surveillance. Officers likely to consider the use of RIP(S)A powers as part of their duties should, therefore, ensure that they are aware of all of the guidance made available.

4.0 Key Definitions

4.1 **Covert surveillance** is any surveillance carried out in a way which is calculated to ensure that the persons who are subject to the surveillance are unaware that it is or may be taking place.

4.2 There are two types of covert surveillance covered by RIP(S)A: **intrusive**, and **directed** surveillance:

4.3 **Intrusive Surveillance** – is defined as:

(i) covert surveillance in relation to anything taking place in any residential premises or in any private vehicle; and

(ii) involves the presence of an individual or surveillance device on the premises or is carried out by means of a device located elsewhere that is capable of providing information of a quality similar to that expected by the presence on the premises or in a vehicle.

Examples include covertly looking in through the windows of residential premises or any private vehicle or directing a camera or any other type of surveillance device into residential premises or private vehicle, to provide information as to what is going on inside.

Officers are reminded that the Council has **no power to authorise or undertake intrusive surveillance**

4.4 Directed Surveillance - The Council only has power to authorise and conduct *directed surveillance* operations

4.5 Definition of Directed Surveillance

Directed surveillance involves surveillance which is covert, but **not intrusive,** and is undertaken for the purpose of a specific and defined investigation or operation. The surveillance must be justified in relation to the likely intrusion of privacy on the target and other individuals, and where appropriate, the need and ability to obtain *private information* ** about a person.

4.6 Directed Surveillance may only be carried out by the Council if it can be shown that the overall purpose of the operation is for:

- the prevention or detection of crime or disorder;
- in the interests of public safety or
- the protection of public health;

4.7 Examples of directed surveillance include covertly looking **at** an area or premises or a vehicle or directing a surveillance device **at, but not into,** premises or a vehicle. In other words directed surveillance relates to situations where someone or some device covertly watches or listens to events which take place **outside** residential premises or **outside** a private vehicle.

(***Private information*** consists of details relating to an individual's private and family life, their home, and their correspondence. The fact that that a covert surveillance operation may take place in a public place (or on business premises) does not mean that that it cannot result in the collecting of private information about an identified person. Prolonged surveillance targeting an individual will, almost without exception, result in the obtaining of private information about him/her and potentially others they come into contact with.

In a similar fashion, where normally overt town centre CCTV cameras are utilised in a covert surveillance operation to, for example, observe commercial premises, private information relating to the way a person operates their business may well be recorded. It is also possible that such an operation will reveal information about their private live and/or the private lives of others.

Officers should therefore note that the term '*private information*' can include information about business and professional activities.

5.0 Authorisation to Conduct a Directed Surveillance Operation.

5.1 Council staff, or those working directly on the Council's behalf, may be permitted to carry out directed surveillance – but only if they follow the authorisation process which the law requires.

5.2 A correct and proper authorisation will provide officers with the legal authority to carry out covert surveillance, enable the collection of evidence, and will reduce the possibility of a legal challenge on both the action, and the admissibility of the evidence collected.

5.3 **Authorisation to carry out directed surveillance may only be given by:**

i. the Chief Executive, or
ii. the Depute Chief Executive, or
iii. the Executive Director

Importantly, and for the avoidance of doubt, this power to authorise may <u>not</u> be further delegated.

6.0 Submitting or Approving an application to carry out a Directed Surveillance Operation

6.1 Officers and Authorising Officers should refer to the Council's guidance on the use of the appropriate forms and the information that will be required before an operation may be considered for authorisation.
(Note - ***Guidance - Applying for/approving Direct Surveillance*** is available on CONNECT, along with the relevant forms).

The authorising officer should also ensure that they have referred to the Office of the Surveillance Commissioner's (OSC) Procedures and Guidance - this document is available from the RIP(S)A Co-ordinating Officer.

7.0 Duties and Responsibilities of Authorisation Officers, the Senior Responsible Officer and the RIP(S)A Co-ordinating Officer

7.1 The level of seniority of the Council's three Authorisation Officers is set deliberately to ensure adequate control and to reflect the seriousness of potential interference with the right of an individual to privacy. Authorising Officers would not be expected to be personally involved in surveillance operations, but for the avoidance of doubt, they must never authorise their own surveillance activities.

7.2 Before an application for directed surveillance can be approved, the authorising officer must determine:
Necessity

- Consideration has been given as to why covert surveillance should be used in the operation;
- The action is necessary and that one of the grounds for approving surveillance is satisfied;
- There is no reasonable and effective alternative way of achieving the desired objective;

Proportionality

- A surveillance operation in principal, and the method of surveillance proposed, is proportionate to the alleged mischief;
- The risk of accidental or collateral intrusion into the privacy of the target and/or others has been assessed, and action has been taken to limit the potential impact.

(Note - please refer to ***Guidance - Applying for/approving Direct Surveillance*** (Section 3.2) for further information on necessity and proportionality).

7.3 Authorisation Officers should note that they may be called upon to explain their judgement and the exercise of their powers in a court.

7.4 As well as the role of an Authorisation Officer, the Chief Executive is also the **Senior Responsible Officer**. In this capacity she is responsible:

- for the integrity of the RIP(S)A process within the Council;
- for compliance with RIP(S)A and its regulatory framework;
- for engagement with the Commissioners and Inspectors and
- for overseeing the implementation of any recommendations made by the OSC and for ensuring that authorisation officers are of the appropriate standard.

7.5 **The RIP(S)A Co-ordinating Officer's** role falls under the remit of the Senior Governance Officer. He is responsible for:

- maintaining the Central Record of Authorisations and collating the original applications/authorisations, reviews, renewals and cancellations;
- the oversight of submitted RIP(S)A documentation to ensure compliance with the legislation and regulations;
- organising RIP(S)A training and
- raising awareness within the Council.

8.0 Time Periods

8.1 Surveillance operations are subject to a number of restrictions in relation to time.

8.2 **Effective period** - The Act requires that an authorisation for directed surveillance will be effective for a period of **three months** from the day it takes effect. When assessing an application, an Authorising Officer must, however, include a note on the form as to the length of time an operation is likely to last before it's objectives can be met. He/she should also state a view as to when a review should be conducted.

8.3 Each application to conduct a surveillance operation should be assessed on its own merits. Should it prove necessary, an authorisation can be renewed to extend the surveillance period provided the renewal application demonstrates the continued need and satisfies the criteria for authorisation. Any renewal must be documented using the corporate form for the purpose, and the signed forms must be lodged with RIP(S)A Co-ordinating Officer within two days. Importantly, authorising officers should add their comments as appropriate to all forms applying for an authorisation renewal.

Renewals must be granted before the expiry date as the renewal will take effect from that date.

8.4 **Review period** – For ongoing operations, Authorising Officers are required to **review all authorisations at intervals of not more than 28 days.** Reviews should take place sooner if possible. The original of all review forms should be lodged with the RIP(S)A Co-ordinating Officer as soon as possible after signing.

8.5 **Cancellation** - Where the Authorising Officer (or an operational officer) considers the continuation of a surveillance operation no longer appropriate, the authorisation should be cancelled immediately by completing the form entitled *Cancellation of Directed Surveillance (DS3 Cancellation)*. The form should be lodged with RIP(S)A Co-ordinating Officer within two days.

8.6 **Under no circumstances may authorisations simply be allowed to lapse into cancellation.** Cancellation is a positive act which removes doubt and confirms that the operation has ended.

8.7 **Verbal Authorisation** – verbal authority for an operation can only be granted in urgent cases, and the urgency must be justified. A verbal authorisation remains **in force for a maximum of 72 hours**. An officer requesting and receiving verbal authorisation should immediately alert the RI(S)A Co-ordinator to the fact, and then move to record the details on the normal application form as soon as possible. The form must be submitted for signature by one of the Authorising Officers as soon as possible.

9.0 Exceptions

9.1 Where covert surveillance (as defined) is planned, ***there are no exceptions to the authorisation procedures.***

9.2 Paragraph 3.2 (above) describes activities that do not meet the definition of *covert surveillance* and hence fall outwith the need for authorisation under the Act.

9.3 General observation forms part of the every day work for some officers and, provided this does not involve systematic surveillance of an individual, authorisation may not be required. **However, if the evidence obtained from an casual observation is to stand scrutiny, it may be necessary to prove that surveillance had not been planned. Wherever there is doubt, authorisation should be sought.**

10.0 Central Register of Authorisations

10.1 The RIP(S)A Co-ordinating Officer will maintain a register of current and past applications for covert surveillance operations (for the avoidance of doubt, the register will include details of applications that have been refused).

.

10.2 The Register will hold the details of the application:

- the type of authorisation;
- the date the authorisation was given;
- name and rank/grade of the authorising officer;
- the unique reference number (URN) of the investigation or operation - this will be issued by the RIP(S)A Co-ordinating Officer;

- the title of the investigation or operation, including a brief description and names of subjects, if known;
- whether the urgency provisions were used, and if so why;
- 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 and
- the date the authorisation was cancelled.

10.3 The process of submitting forms and details to the RIP(S)A Co-ordinating Officer is described in the guidance on authorisations, but it should be noted that the originals of all forms must be submitted to him **within two days of signature.**

10.4 Application & authorisation forms will be held securely with the Central Register and retained for as long as is necessary in relation to any investigation or pending /possible future proceedings.

10.5 **Notwithstanding the above, all forms and related details must be retained until such time as the Surveillance Commissioner's representative has the opportunity to inspect and comment on the details.**

11.0 Security and Retention of Documents.

11.1 Officers must consider the sensitivity of covert surveillance related information and documents before committing to forwarding to a third party.

- Hard copy documents moved via the internal mail system should be enclosed in a sealed package marked *'confidential - for the addressee only'* and should be clearly addressed to a known individual. That individual should be pre-warned to expect the documents so that they can be tracked.
- Wherever possible, hard copy documents should be hand delivered.
- Internally, electronic files containing, or relating to, covert surveillance authorisations may only be shared where adequate security and access controls are in place. Files must not be shared over the open network system but may be shared, for example, through the use of 'viewer restricted' controls.
- Related electronic files should not be sent to a third party as an e-mail attachment unless there is confidence that there are no related security issues**.**

11.2 Each Service must make proper arrangements for the retention, security and eventual destruction, of all copies of authorisation and other documentation having regard to RIP(S)A, the Data Protection Act., and the evidential value of the information.

12.0 Training

12.1 All Authorisation Officers will undertake such training as deemed necessary by the Senior Responsible Officer. All operational officers who may require to seek authorisation for a covert surveillance operation shall undertake such training on the process and implications of RIP(S)A as their Head of Service or Director deem necessary.

13.0 Surveillance Commissioners

13.1 The office of the Surveillance Commissioner has responsibility for overseeing the procedures employed by all authorities engaged in covert surveillance. Part of their role is to periodically examine and audit the records and procedures of authorities, and the Council's Authorisation Officers must be prepared to justify their actions when called upon to do so.

13..2 During periods of inspection, all officers with an involvement in the RIP(S)A authorisation process, or the conduct of surveillance operations should be prepared to make themselves available for interview, and should cooperate with the visiting representative of the Commissioner.

14.0 Policy on Managing Covert Human Intelligence Sources (CHIS)

14.1 Part 2 of this Policy deals with the authorisation of a covert human intelligence source.

Part 2

The Council has power to authorise the use of a covert human intelligence source, where, for example**,** it may become necessary to conceal the identity of a staff member operating as an information source by having them work undercover. Alternatively, there may be situations where the Council may covertly ask another person (not employed by the authority) such as a neighbour (the "source") to obtain information about others and subsequently, without that other person's knowledge, pass that information on to the Council. By their nature, actions of this sort may constitute an interference with an individual's right to privacy, and may give rise to legal challenge as a potential breach of Article 8 of the European Convention on Human Rights and the Human Rights Act 1998 ('the right to respect for private and family life'). Careful planning is therefore essential.

Policy on Managing Covert Human Intelligence Sources (CHIS)

Part 2 of this Policy deals specifically with the authorisation and management of a covert human intelligence source.

It is expected that the Council will consider the use of a CHIS in only very rare and unanticipated circumstances. There is a need, however, to ensure that officers are able to refer to guidance on the process involved. In the main, this section should, therefore, be considered background information.

1.0 Introduction

1.1 A covert human intelligence source (CHIS) is someone who establishes or maintains a relationship for the purpose of obtaining information covertly. The Act (Section 7) states that **a CHIS shall not be used unless** the authorising officer Is satisfied that it is necessary for the purposes of or in the interest of:

- preventing or detecting a crime or disorder,
- public safety, or
- protecting public health.

1.2 The **use** or **conduct** of a CHIS operation is similar to directed surveillance in that requires prior authorisation. (For the avoidance of doubt, it is stressed again that the only officers in the Council with the authority to approve operations are the Chief Executive, the Depute Chief Executive, and the Executive Director. Their authority cannot be delegated). Refer to section 8.2 for authorisation in the use of a juvenile or vulnerable individual as a source.

1.3 In addition to all other issues, authorising officers must be clear on key points when a request for use of CHIS is presented to them. They must:

- Satisfy themselves that the use or conduct of the CHIS is in itself proportionate to what is sought to be achieved
- Satisfy themselves that appropriate arrangements are in place for the safety, management and oversight of the individual acting as the CHIS. Authorising officers should record their satisfaction or otherwise in relation to the risk assessments completed and details relating to safety issues as presented by the officer applying for authorisation.
- Assess the degree of likely intrusion on everyone likely to be affected by the surveillance operation.
- Assess and consider the likelihood of any adverse impact on community confidence that may result from the use of information obtained via use of a CHIS.
- Ensure all related records are kept secure and are inspected only on a 'need to know' basis.

1.4 In all instances where a CHIS operation is considered, advice must be sought from the RIP(S)A Co-ordinating Officer before proceeding.

2.0 Policy Objectives

2.1 The objective of this procedure is to ensure that the Council is in a position to make effective and lawful use of Covert Human Intelligence Sources should the need arise. This procedure should be read in conjunction with the relevant legislation, the Scottish Government's Code of Practice on Covert Human Intelligence Sources ('the Code of Practice') and any guidance which the Office of Surveillance Commissioners may issue from time to time. Copies of the Code of Practice are available for reference on-line (CONNECT), or from the RIP(S)A Co-ordinating Officer.

3.0 Scope of the policy

3.1 This policy applies in all cases where a "Covert Human Intelligence Source" is to be used. Covert Human Intelligence Source (referred to as a **source** as defined by Section 1(7) of the RIP(S)A). A person will be acting as a source if they covertly (i.e. without disclosing their true purpose) establish or maintain a personal or other relationship with another person in order to obtain information from that person or to disclose information obtained from that person or to provide access to information to another person. The definition of a source is not restricted to obtaining private information.

3.2 The Council may therefore use a source in two main ways:

- Members of staff may themselves act as a source by deciding to withhold or conceal their true identity in order to obtain information.

- Alternatively, a member of staff may cultivate a member of the public or employee of a business under investigation to provide them with information on a regular basis. This person will also be acting as a source. In both cases the person or persons being investigated are unaware that this is taking place.

3.3 The policy does not apply in circumstances where members of the public volunteer information as part of their accepted level of civic duty. Nor does it apply where contact points (eg specific phone numbers) are set up to receive anonymous information (a good example might be a 'crimestoppers' type service). Officers should, however, be alert to the fact that someone might become a source as a result of a relationship with the Council that began in this way and, in such a case, authorisation must then be sought.

4.0 Relationship with the Directed Surveillance Procedure

4.1 Where it is envisaged that the use of a source will also be accompanied by directed surveillance then authorisation must also be sought under the Council's policy on directed surveillance as well.

4.2 Where a source wearing or carrying a surveillance device **is invited** into residential premises or a private vehicle, separate authorisation is not required under the surveillance procedures as long as this policy has been followed, and authorisation has been given.

4.3 Where a potential source is themselves subject to surveillance to identify whether they would be an appropriate person to act as a future source this surveillance must be authorised in accordance with the surveillance procedure.

5.0 Lawfulness

5.1 Where planning and making use of a source the same principles as for directed surveillance apply in that a source may only be used where necessary to achieve one or more of the permitted purposes (as identified at section 1.1 above)

5.2 A source should only be **utilised where there is no reasonable and effective alternative** way of achieving the desired objective(s).

5.3 Particular care should be taken if the source is likely to obtain information in a situation where the person under investigation would expect a high degree of privacy.

5.4 Consideration must be given to the extent to which the use and conduct of a source will interfere with the privacy of persons other than the subject of the investigation and to minimise the impact on them. Reasonable steps shall also be taken to minimise the acquisition of information that is not directly necessary for the purposes of the investigation or operation being carried out. If the investigation unexpectedly interferes with the privacy of individuals not covered by the authorisation consideration must be given to whether a new authorisation is required.

5.5 Additionally, the tasking and managing of a source shall be undertaken only by suitably trained or experienced employees, or under their direct supervision.

6.0 Authorisation Procedure

6.1 The use of all sources shall be authorised in accordance with the procedures described below.

a) Authorising officers must not be responsible for authorising their own activities.

b) Where one agency is acting on behalf of another it will normally be the case that the tasking or lead agency shall obtain and provide the authorisation.

c) Authorisations must be given in writing. In really urgent cases only, an Authorising Officer may approve oral applications. Following an oral agreement, an authorisation remains in force for a maximum of 72 hours. An applicant requesting and receiving verbal authorisation should immediately alert the RIP(S)A Co-ordinating Officer to the fact, and then move to record the details on the normal application form as soon as possible. The form must be submitted for signature by one of the Authorising Officers as soon as possible.

d) In accordance with the Code of Practice, authorisations will last for 12 months. The person responsible for authorising the surveillance must ensure that the authorisation is reviewed at least monthly and all authorisations that are no longer needed or appropriate are cancelled.

e) All reviews must be documented using the correct form, available on CONNECT.

f) Reviews must be carried out more frequently where there exists a risk of acquiring confidential material or where the source is a juvenile or deemed vulnerable.

g) All applications (including those that are refused by an authorising officer) **will be recorded in the Central Register.**

7.0 Confidential Material

7.1 Applications **where a significant risk of acquiring confidential material has been identified** shall always require additional scrutiny by the Authorising Officer. Confidential material consists of:

- matters subject to legal privilege (for example between professional legal adviser and client).
- confidential personal information (for example relating to a person's physical or mental health) or confidential journalistic material.

7.2 Such applications shall only be granted in exceptional and compelling circumstances where the authorising officer is fully satisfied that this conduct is both necessary and proportionate in the circumstances.

7.3 Where any confidential material is obtained, the matter must be reported to Office of Surveillance Commissioners during their next regular inspection. Reviews may need to be more regularly carried out than monthly where the source provides access to confidential material or where collateral intrusion exists.

8.0 Vulnerable and Juvenile Sources

8.1 The code of practice defines a vulnerable individual as "*a person who is or may be in need of community care services by reason of mental or other disability, age, illness and who is or may be unable to take care of himself, or unable to protect himself against significant harm or exploitation"* (para 4.13)

8.2 Only the Chief Executive may authorise the use of a vulnerable or juvenile person as a source.

8.3 Particular care must be taken where authorising the use or conduct of vulnerable or juvenile individuals to act as sources. Vulnerable individuals should only be authorised to act as a source in the most exceptional circumstances and, prior to deciding whether or not to grant such approval, the Authorising Officer will seek the advice of the Chief Social Work Officer on the appropriateness of the proposal. If granted.

8.4 For the purposes of this Policy, a juvenile is any person under the age of eighteen. On no occasion should the use of a source under sixteen years of age be authorised to give information against his or her parents or any person who has parental responsibilities for him or her.

8.4 The following conditions must also be met:

- a risk assessment must be undertaken to identify any physical and psychological aspects of their deployment. This risk assessment must be carried out in conjunction with a registered social worker from a relevant discipline i.e. children and families, criminal justice or community care;
- the authorising officer must be satisfied that any risks have been properly explained; and
- the authorising officer must give particular consideration to the fact that the juvenile is being asked to obtain information from a relative, guardian or other person who has assumed responsibility for their welfare.
- An appropriate adult e.g. social worker or teacher must also be present between any meetings between the authority and a source under 16 years of age.
- The maximum authorisation period that can be granted for a juvenile source is one (1) month.

9.0 Management of a Source

9.1 Before authorisation can be given, the authorising officer must be satisfied that suitable arrangements are in place to ensure satisfactory day to day management of the activities of the source and for overseeing these arrangements. An individual officer must be appointed to be responsible for the day to day contact between the source and the authority including:

- Dealing with the source on behalf of the authority
- Directing the day to day activities of the source
- Recording the information supplied by the source
- Monitoring the source's security and welfare

9.2 In addition the authorising officer must satisfy themselves that an officer has designated responsibility for the general oversight of the use made of the source.

9.3 The authorising officer must also ensure that a risk assessment is carried out to determine the risk to the source of any tasking, and the likely consequences if the role of the source becomes known. It will be the responsibility of the officer in day to day control of the source to highlight any concerns regarding their personal circumstances and anything which may **affect the validity of the risk** assessment, the conduct of the source or the safety or welfare of the source.

9.4 Records must also be maintained, in accordance with the relevant Regulations, detailing the use made of the source. It will be the responsibility of the person in day to day control of the activities of the source to maintain the relevant records. The following matters must be included in the records relating to each source:

(i) identity of the source and the means by which the source is referred to
(ii) the date when and the circumstances within the source was recruited
(iii) the name of the person with day to day responsibility for the source and the name of the person responsible for overall oversight
(iv) any significant information connected with the security and welfare of the source
(v) confirmation by the authorising officer that the security and welfare of the source have been considered and any risks have been fully explained and understood by the source
(vi) all contacts between the source and the local authority
(vii) any tasks given to the source
(viii) any information obtained from the source and how that information was disseminated
(ix) any payment, benefit or award or offer of any payment, benefit or award or offer given to a source who is not an employee of the local authority
(x) any relevant investigating authority other than the authority maintaining the records

10.0 Security and Retention of Documents and Materials

10.1 Documents created under this procedure are highly confidential and shall be treated as such. The protection of information must never be less than that afforded to anything related to a directed surveillance operation.

10.2 Services shall make proper arrangements for record retention, security and destruction, in accordance with the requirements of the Data Protection Act 1998, the Code of Practice, and the evidential value in the case.

10.3 All material obtained as a result of the activities of a source must be retained if it is believed that it is relevant to that investigation or to pending or future criminal or civil proceedings. It must be retained until its review suggests that the risk of legal proceedings no longer exists or having taken place has been resolved.

11.0 Avoidance of Doubt.

11.1 for the avoidance of doubt, the following should be noted:

a) **Test Purchasing**. In some cases it has been unclear as to whether or not a source is involved when officers conduct test-purchasing exercises. It is noted that an explicit statutory power may exist under other legislation authorising employees of the Council to carry out activities such as test purchasing.

Where statutory authority exists under other legislation, it will not normally be necessary to seek authorisation under this policy as it is normally the case that those activities do not meet the test required to identify covert surveillance.

However, where the test purchasing activity requires an officer (or other individual) to establish a personal relationship with any person, or where the activity concerned takes place on premises which are also residential, or in a situation where a high degree of privacy would be expected, then authorisation must be sought.

b) **Staffing Matters**. This policy shall not apply to any disciplinary investigation or any activity involving the surveillance of staff of the Council, unless such surveillance directly relates to a regulatory function of the Council.