East Lothian Council

REPORT TO: Cabinet

MEETING DATE: 12 March 2013

BY: Executive Director (Support Service)

SUBJECT: Regulation of Inspectory Powers (RIPSA) Policy

---

1 PURPOSE

1.1 To seek approval from Cabinet of the Regulation of Inspectory Powers (RIPSA) Policy.

2 RECOMMENDATIONS

That Cabinet approve the attached Regulation of Inspectory Powers (RIPSA) Policy and adopt it as Council policy.

3 BACKGROUND

3.1 Prior to this document, East Lothian Council had a policy each for the two aspects of RIPSA – directed surveillance and covert human intelligence sources. The new policy is a more user-friendly single document, which, together with the flowcharts outlining procedures, will provide RIPSA users with clear guidance. The policy will thus assist in ensuring that all surveillance is carried out within the remits of the law and that the results can be used for court proceedings where necessary.

3.2 The Office of the Surveillance Commissioners regularly conducts inspections among local authorities for compliance with the Regulation of Investigatory Powers (Scotland) Act 2000. The next inspection of East Lothian Council has been scheduled for 3 June 2013.

3.3 The Policy has been subject to Corporate Management Team consideration and approval as well as workforce and Trades Unions Consultation. The Policy on RIPSA is not a collective agreement with the Trades Unions.

4 POLICY IMPLICATIONS

4.1 The Policy will provide clarity and consistency of approach for staff, clients and members of the public.

5. EQUALITIES IMPACT ASSESSMENT

5.1 An EQIA has been undertaken and no negative impacts have been identified.

6 RESOURCE IMPLICATIONS

6.1 Financial – None.

6.2 Personnel – The policy will be communicated via Elnet and E-alert to employees of the Council.

6.3 Other – None

7 BACKGROUND PAPERS

7.1 New RIP(S)A Policy

7.2 Old policies

AUTHOR'S NAME	Dr Renate Gertz
DESIGNATION	Data Protection & Freedom of Information Compliance Officer
CONTACT INFO	rgertz@eastlothian.gov.uk ext. 7993
DATE	7 February 2013

7.1.
EAST LOTHIAN COUNCIL

Regulation of Investigatory Powers (Scotland) Act Policy

CONTENTS

PAGE

1. Introduction

1.1 This document sets out East Lothian Council's policy regarding the Regulation of Investigatory Powers (Scotland) Act 2000 (RIPSA).

1.2 In some circumstances, it may be necessary for East Lothian Council employees, in the course of their duties, to make observations of a person or persons in a covert manner, i.e. without that person's knowledge. By their nature, actions of this sort may constitute an interference with that person'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'). RIPSA was enacted to provide a clear statutory framework for the operation of certain intrusive investigative techniques, to provide for compliance with the Human Rights Act 1998 (HRA).

2. Statement of Intent

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 RIPSA, and to set the parameters for expected good practice.

2.2 East Lothian Council is committed to respecting and maintaining citizen's privacy and is fully committed to complying with HRA. Both RIPSA and HRA impact on the way the Council conducts its business. Amongst other things, HRA entitles citizens to expect 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. RIPSA recognises that these rights may, nevertheless, be lawfully infringed in some circumstance provided the method used is lawful, has a legitimate aim, necessary and is proportional to what it would achieve.

3. Objective

The objective of this procedure is to ensure that all covert surveillance by East Lothian Council employees is carried out effectively, while remaining in accordance with the law. It should be read in conjunction with the relevant legislation, the Scottish Government's Code of Practice on Covert Surveillance ('the Code of Practice') and any guidance which the Office of Surveillance Commissioners may issue from time to time.

4. Officers involved

Investigating Officers: officers conducting the surveillance
Authorising Officers: officers authorising the surveillance
Gatekeeper: officer monitoring and approving each authorisation/ cancellation
Senior Responsible Officer (SRO): responsible for strategic overview, main point of contact with the Surveillance Commissioner

5. Types of Surveillance

5.1 Overt Surveillance

Most of the surveillance carried out by East Lothian Council will be done overtly – there will be nothing secretive, clandestine or hidden about it. One way of rendering surveillance overt is by telling the subject that it will happen. Examples of this could be where the alleged perpetrator of a noise nuisance is warned (preferably in writing) that noise will be recorded if the noise continues, or where an entertainment licence is issued subject to conditions and the licensee is told that officers may visit without notice and/or without
identifying themselves to the owner/proprietor to check that the conditions are being met.

5.2 Covert Surveillance

Surveillance will be covert where it is carried out in a manner calculated to ensure that the person or persons subject to the surveillance are unaware that it is or may be taking place. There are two forms covert surveillance can take – directed and intrusive.

Directed Surveillance

Surveillance is directed surveillance if the following criteria are met:

- it is covert, but not intrusive, surveillance;
- it is conducted for the purposes of a specific investigation or operation;
- it is likely to result in the obtaining of private information about a person (whether or not one specifically identified for the purposes of the investigation or operation);
- it is conducted otherwise than by way of an immediate response to events orcircumstances, the nature of which are

such that it would not be reasonably practicable for an *authorisation* under Part II of the 2000 Act to be sought.

Intrusive Surveillance

Covert surveillance is intrusive if it is carried out:

- in relation to anything taking place in any residential premises or in any private vehicle; and
- involves the presence of an individual on the premises or alternatively the use in vehicle or residential premises of any surveillance device.

Intrusive surveillance can only be carried out only by police and other law enforcement agencies.

5.3 Covert Human Intelligence Sources (CHIS)

A person is a CHIS if:
(a) s/he establishes or maintains a personal or other relationship with a person for the covert purpose of facilitating the doing of anything falling within paragraphs (b) or (c) below;
(b) s/he covertly uses such a relationship to obtain information or to provide access to any information to another person; or
(c) s/he covertly discloses information obtained by the use of such a relationship or as a consequence of the existence of such a relationship.

A local authority may use a CHIS in two main ways:

- Employees of East Lothian Council may themselves act as a source by failing to disclose their true identity in order to obtain information.
- Alternatively an employee of East Lothian Council may cultivate a member of the public or employee of a business under investigation to provide them with information on a regular basis.

In both cases the person or persons being investigated are unaware that this is taking place. The procedure does not apply in circumstances where members of the public volunteer information as part of their normal civic duties or contact numbers specifically set up to receive anonymous information such as crimestoppers; nor do they become a CHIS if they are asked if they can provide additional information, e.g. details of the suspect's vehicle or the time that they leave for work.

However, someone might become a CHIS as a result of a relationship with East Lothian Council that began in this way and authorisation must then be sought.

5.4 Examples of different types of surveillance

Type of Surveillance	Examples
Overt	• Police Officer or Dog Warden on patrol • Sign-posted town centre CCTV • Recording noise coming from premises after occupier has been warned that this would occur • Most test purchases
Covert but not requiring prior authorisation	• CCTV cameras providing general traffic information
Directed surveillance must be RIPSA authorised CHIS must be RIPSA authorised	• Officers follow an individual over a period to establish whether s/he is working while claiming benefit • Noise recording from neighbour's premise without occupier of premise from which noise emanates having been warned • Test purchases where the officer will be establishing a relationship for a covert operation
Intrusive	• Planting a listening or other device in a person's home or private vehicle

6. Authorisation for Directed Surveillance

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

6.2 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.

6.3 Authorisation to carry out directed surveillance may only be given by the Authorising Officers:

- Executive Directors

- Designated Heads of Service
- Designated Senior Managers

6.4. Applications for authorisation must be in writing using the authorisation form in Appendix C (Copies of all forms are available on EL*Net* at: http://elnet.eastlothian.gov.uk/site/scripts/downloads.php?categoryID=20556)
All such requests must be submitted to an Authorising Officer of the Council. All requests must be considered and authorised in writing by an Authorising Officer, before any covert surveillance operation can commence. Authorisation will only be granted where covert surveillance is believed by the Authorising Officer to be necessary and proportionate. Once the request has been authorised, it will be sent to the Gatekeeper for monitoring and approval. Once the request is thus approved, surveillance will commence. All forms will be stored securely by the Gatekeeper. Procedural details can be found in Appendix A.

6.5. RIPSA stipulates that the Authorising Officer must believe that the activities to be authorised are necessary on one or more statutory grounds. These grounds are:

- For the purpose of preventing or detecting crime or of preventing disorder
- In the interests of public safety
- For the purpose of protecting public health

If the activities are deemed necessary on one of more of these statutory grounds, the Authorising Officer must also believe that they are proportionate to what is sought to be achieved by carrying them out. This involves balancing the seriousness of the intrusion into the privacy of the subject of the operation (or any other person who may be affected) against the need for the activity in investigative and operational terms.

The authorisation will not be proportionate if it is excessive in the overall circumstances of the case. Each action authorised should bring an expected benefit to the investigation or operation and should not be disproportionate or arbitrary. The fact that a suspected offence may be serious will not render intrusive actions proportionate. Similarly, an offence may be so minor that any deployment of covert techniques would be disproportionate. No activity should be considered proportionate if the information which is sought could reasonably be obtained by other less intrusive means.

The following elements of proportionality should therefore be considered:

- balancing the size and scope of the proposed activity against the gravity and extent of the perceived crime or offence;
- explaining how and why the methods to be adopted will cause the least possible intrusion on the subject and others;
- considering whether the activity is an appropriate use of the legislation and having considered all reasonable alternatives, a reasonable way of obtaining the necessary result;
- evidencing, as far as is reasonably practicable, what other methods have been considered and why they were not implemented.

It is important therefore that all those involved in undertaking directed or intrusive surveillance activities or interference with property under RIPSA are fully aware of the extent and limits of the authorisation or warrant in question.

6.5 Collateral Intrusion

An application for an authorisation should include an assessment of the risk of any collateral intrusion, i.e. the extent to which the surveillance will interfere with the privacy of persons other than the subject of the surveillance and to minimise the impact of the surveillance on them. The authorising officer should take this into account, when considering the proportionality of the use and conduct of a source. 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.

6.6 Confidential Information

The possibility of coming across confidential information during a surveillance operation must always be given proper consideration before any applications are authorised. This consists of:

- Matters subject to legal privilege - for example oral and written communications between a professional legal adviser and his client or any person representing his client, made in connection with the giving of legal advice to the client or in contemplation of legal proceedings and for the purposes of such proceedings, as well as items enclosed with or referred to in such communications. Communications and items held with the intention of furthering a criminal purpose are not

subject to legal privilege where there is evidence that the professional legal advisor is intending to hold or use them for a criminal purpose.

- Confidential personal information - which is information held inconfidence concerning an individual (living or dead) who can be identified from it, and relating to a) his physical or mental health or b) to spiritual counselling or other assistance given or to be given, and which a person has acquired or created in the course of any trade, business, profession or other occupation, or for the purposes of any paid or unpaid office. It includes oral and written information and also communications as a result of which personal information is acquired or created. Information is held in confidence if it is subject to a restriction on disclosure or an obligation of secrecy contained in exiting or future legislation
- Confidential journalistic material - which includes material acquired or created for the purposes of journalism and held subject to an undertaking to hold it in confidence, as well as communications resulting in information being acquired for the purposes of journalism and held subject to an undertaking.

7. Urgent Authorisations

Urgent authorisations should not normally be necessary. In exceptional circumstances, however, urgent authorisations may be given orally if the time that would elapse before a written authorisation can be granted would either be likely to (1) endanger life or (2) jeopardise the investigation or operation for which the authorisation was being given. Urgent authorisations will normally only be given following consultation with the SRO or the Chief Executive.

An application will never be urgent where the need for authorisation has been neglected or is of the Applicant's own making.

Urgent authorisations last for no more than 72 hours.

Where authorisations are granted orally under urgency procedures, a record detailing the actions authorised and the reasons why the urgency procedures were used should be recorded by the Applicant and Authorising Officer as a priority.

8. Duration of Authorisations

8.1 A written authorisation must state the length of time an operation is likely to last before its objectives can be met. This should be as short as possible, but must not exceed a maximum of three months_from the day it takes effect. A three-month authorisation may be considered the norm where it appears necessary, otherwise authorisation should be for the shortest time in which it may be possible to collect the required evidence, or to evaluate continuation of the operation.

8.2 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. Details of the review and decision reached are to be noted on the appropriate form, approved by and lodged with the Gatekeeper within two days.

8.3 Where the authorising 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* (see Appendix C). The form should be approved by and lodged with the Gatekeeper within two days. 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.

9. Authorisation for Covert Human Intelligence Sources

9.1 Both the conduct and/or use of a CHIS require prior authorisation:

- The use of a CHIS involves any action on behalf of a public authority to induce, ask or assist a person to engage in the conduct of a CHIS, or to obtain information by means of the conduct of a CHIS. In general, therefore, an authorisation for use of a CHIS will be necessary to authorise steps taken by a public authority in relation to a CHIS.
- The conduct of a CHIS is any conduct of a CHIS which falls within paragraph F (1) (a) to (c) above or is incidental to anything falling within that paragraph. In other words, an authorisation for conduct will authorise steps taken by the CHIS on behalf of, or at the request of a public authority.

Care should be taken to ensure that the CHIS is clear on what is/is not authorised at any given time and that all the CHIS's activities are properly risk assessed. Care should also be taken to ensure that relevant applications, reviews, renewals and

cancellations are correctly performed. A CHIS may in certain circumstances be the subject of different use or conduct authorisations obtained by one or more public authorities. Such authorisations should not conflict.

9.2 East Lothian Council will ensure that arrangements are in place for the proper oversight and management of CHIS, including appointing individual officers as defined in Section 7(6)(a) of RIPSA for each CHIS. The person referred to in Section 7(6)(a) of the 2000 Act, the "handler", will have day to day responsibility for:

- dealing with the CHIS on behalf of the authority concerned;
- directing the day to day activities of the CHIS;
- recording the information supplied by the CHIS; and
- monitoring the CHIS's security and welfare.

The handler of a CHIS will usually be of rank or position below that of the authorising officer.

9.3 The same principles and procedures apply for the authorisation of a CHIS as for directed surveillance – use of a CHIS must be necessary and proportionate. Also, the possibility of collateral intrusion or of obtaining confidential information must be taken into account.

9.4 Use of a CHIS may only be authorised if it is necessary for the prevention or detection of crime or the prevention of disorder; in the interests of public safety; for the purpose of protecting public health; or for any other purpose prescribed in an order made by the Scottish Ministers.

9.5 Applications to use, extend or discontinue the use of a CHIS must be made in writing on the Council's corporate forms, as set out in Appendix D. Exceptionally, an oral authorisation may be granted for the use of a CHIS in circumstances of urgency. As with directed surveillance, Authorising Officers are responsible for ensuring that authorisation is cancelled as soon as it is no longer required, and that reviews of authorisations are carried out on at least a monthly basis.

9.6 An application for authorisation for the use or conduct of a source should be in writing and record:

- the reasons why the authorisation is necessary in the particular case and on the grounds (e.g. for the purpose of

preventing or detecting crime) listed in section 7(3) of the RIP(S) Act;
- the reasons why the authorisation is considered proportionate to what it seeks to achieve;
- the purpose for which the source will be tasked or deployed (e.g. in relation to an organised serious crime, espionage, a series of racially motivated crimes etc);
- where a specific investigation or operation is involved, nature of that investigation or operation;
- the nature of what the source will be tasked to do;
- the level of authority required (or recommended, where that is different);
- the details of any potential collateral intrusion and why the intrusion is justified;
- the details of any confidential information that is likely to be obtained as a consequence of the authorisation; and a subsequent record of whether authority was given or refused, by whom and the time and date.

9.7 The following matters must be included in the records relating to each and every source:

- the identity of the source;
- the identity, used by the source (if known/applicable);
- any relevant investigating authority other than the authority maintaining the records;
- the means by which the source is referred to within each relevant investigating authority;
- any other significant information connected with the security and welfare of the source;
- any confirmation made by a person granting or renewing an authorisation
- for the conduct or use of a source that any identified risks to the security and welfare of the source have, where appropriate, been properly explained to and the date when, and the circumstances in which, the source was recruited;
- the identities of the persons who, in relation to the source, are discharging or have discharged the functions mentioned in section 7(6)(a) to (c) of the 2000 Act or in any order made by the Scottish Ministers under section 7(4)(b)
- the periods during which those persons have discharged those responsibilities;
- the tasks given to the source and the demands made of him in relation to his activities as a source;
- all contacts or communications between the source and a person acting on behalf of any relevant investigating authority;

- the information obtained by each relevant investigating authority by the conduct or use of the source;
- any dissemination by that authority of information obtained in that way; and
- 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.

9.8 Special safeguards apply to the use or conduct of juvenile sources (i.e.under 18 year olds) and a child under 16 years of age cannot be authorised to give information against his or her parents. In other cases, authorisations should not be granted unless the special provisions contained within The Regulation of Investigatory Powers (Juveniles) (Scotland) Order 2002; SSI No. 206 are satisfied. Only the Chief Executive and in his/her absence a Chief Officer is authorised by the Council to permit the use of juvenile sources and this will only occur in exceptional circumstances.

9.9 Similarly, special provisions apply to vulnerable individuals. 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 or herself, or unable to protect himself or herself against significant harm or exploitation. A vulnerable individual will only be authorised to act as a source in the most exceptional of circumstances. Only the Chief Executive and in his/her absence a Chief Officer is authorised by the Council to permit the use of vulnerable individuals and this will only occur in exceptional circumstances.

9.10 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.

9.11 CHIS authorisations must be reviewed regularly to assess the need for the use of a source to continue. Reviews should include the use made of the source during the period authorised, the tasks given to the source and the information obtained from the source. The results of a review should be recorded on the authorisation record. There is no set time frame for reviews, however, the authorising officer should determine how often a review should take place. This should be as frequently as is considered necessary and practicable.

9.12 Before an authorisation is renewed, the authorising officer must be satisfied that a review of the use of the source has been carried out.
If the authorising officer considers it necessary for the authorisation to continue for the purpose for which it was given, he may then renew it in writing. Renewals may also be granted orally in urgent cases. A renewal takes effect at the time at which, or day on which the authorisation would have ceased to have effect. An application for renewal should not be made until shortly before the authorisation period is drawing to an end. Any authorising officer can renew an authorisation. Authorisations may be renewed more than once, if necessary, provided they continue to meet the criteria for authorisation. The renewal should be kept/recorded as part of the authorisation record.

9.13 If the use or conduct of the source no longer satisfies the criteria for authorisation or if satisfactory arrangements for the source's case no longer exist, the authorising officer who granted or renewed the authorisation must cancel it. If the authorising officer is no longer available, the person who has taken over the role of authorising officer or the person who is acting as authorising officer must cancel the authorisation. (see The Regulation of Investigatory Powers (Cancellation of Authorisations) (Scotland) Order 2002; SSI No. 207). Where necessary, the safety and welfare of the source should continue to be taken into account after the authorisation has been cancelled.

10. Duration of Authorisations for Covert Human Intelligence Sources

10.1 A written authorisation must state the length of time an operation is likely to last before its objectives can be met. This should be as short as possible, but must not exceed a maximum of 12 months from the date of authorisation or

extension. If a juvenile CHIS is used, the duration of such an authorisation is one month instead of twelve months.

10.2 Urgent oral authorisations or authorisations granted or renewed by a person who is entitled to act only in urgent cases will, unless renewed, cease to have effect after seventy-two hours, beginning with the time when the authorisation was granted or renewed. Urgent oral authorisations will be subject to the same requirements as that set out above relating to directed surveillance.

10.3 Authorisations can be renewed for a further period of twelve months. Renewals may also be granted orally in urgent cases and last for a period of seventy-two hours.

11. Records Management

11.1 A central record of all Authorisations, Reviews, Renewals, Cancellations and rejections will be maintained and monitored by the Gatekeeper. Each form will have a unique reference number (URN). The cross-referencing of each URN takes place within the Forms for audit purposes. Rejected Forms will also have URN's.

11.2 Authorising Officers must scan and forward the original copies of each Form to the Gatekeeper for storage. The records will be retained in the Central Register for a period of at least three years from the ending of the authorisation and will be securely held in electronic format.

11.3 The following documents must be securely retained by the Applicant.

- a copy of the Forms together with any supplementary documentation
- (including Risk Assessments carried out prior to authorisation);
- notification of the approval given by the Authorising Officer;
- the Unique Reference Number for the authorisation (URN) assigned to it by the person maintaining the Central Register (who should be applied to whilst the application is being completed);
- a record of the period over which the surveillance has taken place;
- the frequency of reviews prescribed by the Authorising Officer;
- a record of the result of each review of the authorisation;

- 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;
- a copy of the cancellation of the surveillance

12. Training

All Authorising and Investigating Officers are required to undergo regular training provided by the Gatekeeper to ensure that the requirements of the law are complied with.

13. Surveillance Commissioners

The office of the Chief Surveillance Commissioner has responsibility for overseeing the procedures employed by all authorities engaged in covert surveillance. Part of its 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.

14. Complaints

Any person who reasonably believes that they have been adversely affected by any activities carried out pursuant to this policy by or on behalf of the Council may complain to the Feedback Team/Senior Responsible Officer who will investigate the complaint. Such a person may also complain to the Investigatory Powers Tribunal at:

Investigatory Powers Tribunal
PO Box 33220
London
SW1H 9ZQ

15. Review of Policy

This policy will be reviewed every three years from the date of approval.

7.2.

East Lothian Council

Procedure for Authorisation of Covert Surveillance

1. Foreword

1.1 The use of surveillance to provide information is a valuable resource for the protection of the public and the maintenance of law and order. In order that local authorities and law enforcement agencies are able to discharge their responsibilities, use is made of unaided surveillance and surveillance devices. Where this surveillance is covert i.e. the subject of the surveillance is unaware that it is taking place, then it must be authorised to ensure that it is lawful. CCTV systems in the main will not be subject to this procedure as they are 'overt' forms of surveillance. However where CCTV is used as part of a pre-planned operation of surveillance then authorisation should be obtained.

1.2 Until October 2000 covert surveillance was not subject to statutory control in the UK. From that date a legal framework ensures that the use of surveillance is subject to an authorisation, review and cancellation procedure.

2. Policy statement

2.1 In some circumstances, it may be necessary for East Lothian Council employees, in the course of their duties, to make observations of a person or person(s)in a covert manner, i.e. without that person's knowledge. By their nature, actions of this sort may constitute an interference with that person'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').

2.2 The Regulation of Investigatory Powers Act (2000) [RIPA] and the Regulation of Investigatory Powers (Scotland) Act (2000) [RIP (S) A] ('the Acts') together provide for the first time a legal framework for covert surveillance activities by public authorities (including local authorities) and an independent inspection regime to monitor these activities.

Whilst the Acts do not impose a requirement for local authorities to seek or obtain an authorisation, where one is available East Lothian Council employees will adhere to the authorisation procedure before conducting any covert surveillance. East Lothian Council will comply with the terms of the Code of Practice issued by the Scottish Ministers under section 24(1) of RIPA 2000

which came into force on the 11th March 2003. That code of practice is admissible as evidence in criminal and civil proceedings and must be taken into account by any court or tribunal concerning evidence in civil and criminal proceedings obtained by covert surveillance where it appears relevant to them.

2.4 Employees of East Lothian Council will **not** carry out intrusive surveillance within the meaning of the Regulation of Investigatory Powers (Scotland) Act 2000. This is surveillance of anything taking place on residential premises or in a private vehicle that involves the presence of an individual on the premises or in the vehicle or is carried out by means of a surveillance device capable of providing information of the same quality and detail as might be expected to be obtained from a device actually present on the premises or in the house.

3. Objective

3.1 The objective of this procedure is to ensure that all work involving directed surveillance by East Lothian Council employees is carried out effectively, while remaining in accordance with the law. It should be read in conjunction with the Regulation of Investigatory Powers (Scotland) Act 2000 and the Scottish Executive's Code of Practice on the Use of Covert Human Intelligence Sources and the Code of Practice on Covert Surveillance.

3.2 Definitions

3.2.1 **Covert surveillance** means surveillance that is carried out in a manner calculated to ensure that the persons subject to the surveillance are unaware that it is taking place.

3.2.2 **Authorising officer** is the person who is entitled to give an authorisation for directed surveillance in accordance with section 5 of the Regulation of Investigatory Powers (Scotland) Act 2000.

3.2.3 **Private information** includes information about a person relating to his private or family life.

3.2.4 **Residential premises** means any premises occupied or used, however temporarily, for residential purposes or otherwise as living accommodation.

3.2.5 **Private vehicle** means any vehicle that is used primarily for the private purpose of the person who owns it or of a person otherwise having the right to use it. This does not include a person whose right to use a vehicle derives only from his having paid, or undertaken to pay, for the use of the vehicle and its driver for a particular journey. A vehicle includes any vessel, aircraft or hovercraft.

4. Scope of the Procedure

4.1 This procedure applies in all cases where 'directed surveillance' is being planned or carried out. Directed surveillance is defined in the Code of Practice as surveillance undertaken "for the purposes of a specific investigation or operation" and "in such a manner as is likely to result in the obtaining of private information about a person."

4.2 The procedure does not apply to:

Ad-hoc covert observations that do not involve the systematic surveillance of specific person(s)
Observations that are not carried out covertly, or
Unplanned observations made as an immediate response to events.

4.3 In cases of doubt, the authorisation procedures described below should be followed.

5. Principles of Surveillance

5.1 In planning and carrying out covert surveillance, East Lothian Council employees shall comply with the following principles.

5.2 Lawful purposes

Directed surveillance shall only be carried out where necessary to achieve one or more of the permitted purposes (as defined in the Acts) namely:

5.2.1. For the purpose of preventing or detecting crime or the prevention of disorder;
5.2.2 In the interests of public safety;
5.2.3 For the purpose of protecting public health;
5.2.4 For any other purpose prescribed in an order made by the Scottish Ministers.

Employees carrying out surveillance shall not interfere with any property or harass any person.

5.3 Confidential material

5.3.1 Applications where a significant risk of acquiring confidential material has been identified shall always require the approval of **the Chief Executive or in his absence a Director.**

5.3.2 Confidential material consists of:

Matters subject to legal privilege (for example between professional legal advisor and client), or

Confidential personal information (for example relating to a person's physical or mental health) or

Confidential journalistic material.

5.3.3. Where those carrying out authorised surveillance become aware that the operation or surveillance unexpectedly interfere with the privacy of individuals or where confidential or religious material is unexpectedly obtained they will as soon as is reasonably practicable advise their authorising officer or the person set out in para 5.3.1 above as appropriate. The authorising officer will review the authorisation and cancel it where appropriate. Where the current authorisation did not cover the matters encountered a fresh application for authorisation may be submitted.

6. The Authorisation Process

6.1 Applications for Directed Surveillance will be authorised at the level of Investigations Manager or Assistant Head of Service as prescribed by the Regulation of Investigatory Powers (Prescription of Offices, Ranks and Positions) (Scotland) Order 2000. (SI 2000:343 as amended.) For the purposes of East Lothian Council the Investigations Manager will be no lower than fourth tier level and the Assistant Head of Service no lower than third tier level. For public authorities there are no substitutes of lower grade officers prescribed to authorise 'urgent' cases in contrast, for example, to the police.

6.2 Authorising officers within the meaning of this procedure should avoid authorising their own activities wherever possible and only do so in exceptional circumstances.

Authorisations will be in writing. However, in urgent cases a third tier level Manager or Head of Service or above may approve applications orally.

6.4 All applications for directed surveillance authorisations will be made on form **ELC/DSA** The applicant in all cases should complete this. In urgent cases the authorising officer may give an oral authorisation. A statement that the authorising officer has expressly granted the authorisation should be recorded on the form or, if that is not possible, in the applicant's notebook or diary. This should be done by the person to whom the authorising officer spoke (normally the applicant) but should later be endorsed by the authorising officer.

6.5 All applications for directed surveillance renewals will be made on form **ELC/DSR**. The applicant in all cases should complete this where the surveillance requires to continue beyond the previously authorised period (including previous renewals).

6.6 Where authorisation ceases to be either necessary or appropriate the authorising officer or appropriate deputy will cancel an authorisation using form **ELC/CAN**.

6.7 Forms, codes of practice and supplementary material will be available from the Council Intranet and will be maintained by Trading Standards and Legal and Committee Services.

6.8 Any person giving an authorisation for the use of directed surveillance must be satisfied that:

Account has been taken of the likely degree of intrusion into the privacy of persons other than those directly implicated in the operation or investigation ('collateral intrusion'). Measures must be taken, wherever practicable, to avoid unnecessary intrusion into the lives of those affected by collateral intrusion.

The authorisation is necessary.

The authorised surveillance is proportionate.

6.9 Necessity

Surveillance operations shall only be undertaken where there is no reasonable and effective alternative way of achieving the desired objective(s).

6.10 Effectiveness

Surveillance operations shall be undertaken only by suitably trained or experienced employees, or under their direct supervision.

6.11 Proportionality

The use of surveillance shall not be excessive i.e. it shall be in proportion to the significance of the matter being investigated.

6.12 Authorisation

All directed surveillance shall be authorised in accordance with this procedure.

6.13 Use of Directed Surveillance with technical equipment

6.13.1 Where directed surveillance requires the use of a surveillance device and the person carrying out directed surveillance is invited into residential premises or a private vehicle it does not require special authorisation to record activity taking place inside the premises or vehicle. Authorisation for the use of that directed surveillance may be obtained in the usual way.

6.13.2 Applicants should apply within their own line management structure unless other arrangements have been agreed or it is unreasonable or impractical in the circumstances.

6.13.3 Services wishing to adopt a more devolved authorisation process may do so only on the explicit approval of a written policy by the Council; all authorisations must remain within the scope of the Scottish Executive's guidance on authorising grades.

Time Periods – Authorisations

7.1 Oral applications expire after 72 hours beginning with the time the authorisation was originally granted or renewed whichever is the later. If required they can be renewed for a further period of 3 months if renewed in writing.

7.2 Written authorisations expire 3 months from the day on which they took effect.

Time Periods – Renewals

8.1 If at any time before an authorisation would expire (including oral authorisations) the authorising officer considers it necessary for the authorisation to continue for the purpose for which it was given, it may be renewed in writing for a further period of 3 months beginning with the day on which the previous authorisation ceases to have effect. Applications should only be made shortly before the authorisation is due to expire.

Any person entitled to authorise may renew authorisations. They may be renewed more than once, provided they continue to meet the criteria for authorisation.

Review

9.1 The Authorising Officer shall review all authorisations at intervals of not more than one month. Details of the review and the decision reached shall be noted on the original application. More frequent reviews may take place at intervals to be determined by the authorising officer where the surveillance involves collateral intrusion or access to confidential information.

Cancellation

10.1 The authorising officer or appropriate deputy must cancel an authorisation if he/she is satisfied that the directed surveillance no longer satisfies the criteria for authorisation.

Monitoring

11. Each Service or discrete location within Services must maintain a record of all applications for authorisation (including refusals), renewals, reviews and cancellations. The most senior authoriser in that Service or at that location will maintain the monitoring sheet form **ELC/ MS/ripsa.**

12. Security and Retention of Documents

12.1 Documents created under this procedure are highly confidential and shall be treated as such. Services shall make proper arrangements for their retention, security and destruction, in accordance with the requirements of the Data Protection Act 1998 and the Code of Practice.

The Head of Policy and Business management will maintain the Central Register of Authorisations. Authorising officers shall notify, the said Head of the grant, renewal or cancellation of any authorisations and the name of the Applicant Officer within 24 hours to ensure the accuracy of the Central Register. Copies of the forms dealing with the grant, renewal or cancellation of any authorisations will be sent within the same period of time to the said Head.

12.3 The Authorising Officer shall retain the original Authorisation and Renewal forms until cancelled. On cancellation, the original Application, Renewal and Cancellation forms shall be forwarded to the Head of Policy and Business management with the Authorising Officer retaining a copy.

12.4 The Authorising Officer shall retain the copy forms for at least one year after cancellation. The Head of Policy and Business management will retain the original forms for at least three years after cancellation. In both cases these will not be destroyed without the authority of the authorising officer if practicable. Where the evidence from a surveillance operation is likely to be required for civil or criminal proceedings legal advice should be sought prior to any destruction.

13. Oversight

The Office of Surveillance Commissioners (OSC) provides independent oversight of the use of the powers contained within the Regulation of Investigatory Powers (Scotland) Act 2000. This oversight includes inspection visits by Inspectors appointed by the OSC.

14. Complaints

14.1 The Regulation of Investigatory Powers Act 2000 (the ‘UK Act) establishes an independent Tribunal. This has full powers to investigate and decide any cases within its jurisdiction.

EAST LOTHIAN COUNCIL

Procedure for Authorisation of the Use of Covert Human Intelligence Source

1. Foreword

The use of human beings to provide information ('informants') is a valuable resource for the protection of the public and the maintenance of law and order. In order that local authorities and law enforcement agencies are able to discharge their responsibilities, use is made of 'undercover' officers and informants. These are referred to as 'covert human intelligence sources' or 'sources' and the area of work of undercover officers and informants to whom this procedure applies will be referred to as 'source work.'

Until October 2000 the use of such sources was not subject to statutory control in the UK. From that date a legal framework ensures that the use, deployment, duration and effectiveness of sources is subject to an authorisation, review and cancellation procedure.

2. Policy statement

2.1 In some circumstances it may be necessary for East Lothian Council employees, in the course of their duties, to make use of informants and to conduct 'undercover' operations in a covert manner, i.e. without a person's knowledge. By their nature, actions of this sort may constitute an interference with that person'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').

2.2 The Regulation of Investigatory Powers Act (2000) [RIPA] and the Regulation of Investigatory Powers (Scotland) Act (2000) [RIP (S) A] ('the Acts') together provide for the first time a legal framework for covert surveillance and the use of covert human intelligence sources by public authorities (including local authorities) and an independent oversight regime to monitor these activities.

2.3 Whilst the Acts do not impose a requirement for local authorities to seek or obtain an authorisation, where one is available East Lothian Council employees will adhere to the authorisation procedure before using a source or allowing or conducting an undercover operation.

2.4 East Lothian Council will comply with the terms of the Covert Human Intelligence Sources Code of Practice issued by the Scottish Ministers under section 24(1) of RIPA 2000 which came into force on the 11th March 2003. That

code of practice is admissible as evidence in criminal and civil proceedings and must be taken into account by any court or tribunal concerning evidence in civil and criminal proceedings obtained by covert surveillance where it appears relevant to them.

2.5 Employees of East Lothian Council will not carry out intrusive surveillance within the meaning of the Regulation of Investigatory Powers (Scotland) Act 2000 nor will they authorise any person for any covert human intelligence source activity to install any surveillance equipment into residential premises or private vehicle.

3. Objective

3.1 The objective of this procedure is to ensure that all work involving the use or conduct of a source by East Lothian Council employees is carried out effectively, while remaining in accordance with the law. It should be read in conjunction with the Regulation of Investigatory Powers (Scotland) Act 2000 and the Scottish Executive's Code of Practice on the Use of Covert human intelligence sources and the Code of Practice on Covert Surveillance.

Definitions

3.2.1 Covert human intelligence source means a person who establishes or maintains a personal or other relationship with another person for the covert purpose of facilitating anything that:

covertly uses such a relationship to obtain information or to provide 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.

A relationship is used covertly if, and only if, it is conducted in a manner calculated to ensure that the person is unaware of its purpose.

3.2.2 Directed surveillance is defined in the Code of Practice as surveillance undertaken "for the purposes of a specific investigation or operation" and "in such a manner as is likely to result in the obtaining of private information about a person."

3.2.3 Authorising officer is the person who is entitled to give an authorisation for the use or conduct of a source in accordance with section 5 of the Regulation of Investigatory Powers (Scotland) Act 2000.

3.2.4 Handler means the person referred to in section 4(6)(a) of the Regulation of Investigatory Powers (Scotland) Act 2000 holding an office or position within the local authority and who will have day to day responsibility for:

Dealing with the source on behalf of the local authority;

DIRECTING THE DAY TO DAY ACTIVITIES OF THE SOURCE;

Recording the information supplied by the source; and
Monitoring the source's security and welfare.

3.2.5 Controller means the person/the designated managerial officer within the local authority referred to in section 4(6) (b) of the Regulation of Investigatory Powers (Scotland) Act 2000, responsible for the general oversight of the use of the source.

3.2.6 The conduct of a source is action of that source, falling within the terms of the Regulation of Investigatory Powers (Scotland) Act 2000, or action incidental to it.

The use of a source is any action to induce, ask or assist a person to engage in the conduct of a source or to obtain information by means of an action of the source.

Private information includes information about a person relating to his private or family life.

Residential premises means any premises occupied or used, however temporarily for residential purposes or otherwise as living accommodation.

Private vehicle means any vehicle that is used primarily for the private purpose of the person who owns it or of a person otherwise having the right to use it. This does not include a person whose right to use a vehicle derives only from his having paid, or undertaken to pay, for the use of the vehicle and its driver for a particular journey. A vehicle includes any vessel, aircraft or hovercraft.

4. Scope of the Procedure

4.1 This procedure applies in all cases where the use of an undercover officer or source is being planned or carried out.

4.2 This procedure does not apply to:

Covert test purchase transactions under existing statutory powers where the officers involved do not establish a personal or other relationship for the purposes stated (see definition of a covert human intelligence source). As an example the purchase of music CD for subsequent expert examination would not require authorisation but where the intention is to ascertain from the seller where he buys suspected fakes, when he takes delivery etc. then authorisation should be sought beforehand.

Tasks given to persons (whether that person is an employee of the Council or not) to ascertain purely factual information (for example the location of cigarette vending machines in licensed premises).

In cases of doubt, the authorisation procedures described below should be followed.

5. Principles of use or conduct of covert human intelligence source

5.1 In planning and carrying out source work, East Lothian Council employees shall comply with the following principles.

5.2 Lawful purposes

Source work shall only be carried out where necessary to achieve one or more of the permitted purposes (as defined in the Acts) namely:

For the purpose of preventing or detecting crime or the prevention of disorder;
In the interests of public safety;
For the purpose of protecting public health;
For any other purpose prescribed in an order made by the Scottish Ministers.

Employees carrying out source work or using sources must be aware that a source has no licence to commit crime. Any source that acts beyond the acceptable limits of case law in regard to this principle risks prosecution.

5.3 **Confidential material**

5.3.1 Applications where a significant risk of acquiring confidential material has been identified shall always require the approval of The Chief Executive or in his absence a Director.

5.3.2 Confidential material consists of:

Matters subject to legal privilege (for example between professional legal advisor and client),
Confidential personal information (for example relating to a person's physical or mental health) or
Confidential journalistic material.

5.4 **Vulnerable individuals**

5.4.1 Vulnerable individuals, such as the mentally impaired, will only be authorised to act as a source in the most exceptional circumstances. Authorisation of a Director or Chief Executive will be required.

]

5.5 **Juvenile sources**

5.5.1 The use or conduct of any source under 16 years of age living with their parents cannot be authorised to give information about their parents.

5.5.2 Juvenile sources can give information about other members of their immediate family in exceptional cases. A parent, guardian or other 'appropriate adult' should be present at meetings with the juvenile source under the age of 16 years.

5.5.3 The authorisation should not be granted unless or until:

The safety and welfare of the juvenile has been fully considered;
The authorising officer has satisfied himself/herself that any risk has been properly explained and understood by the juvenile;
A risk assessment has been undertaken as part of the application to deploy a juvenile source, covering the physical dangers and the moral and psychological aspects of his or her deployment.

5.5.4 Deployment of juvenile sources will only be authorised by a Director or The Chief Executive.

6. The Authorisation Process

6.1 Applications for the use or conduct of a source will be authorised at the level of Investigations Manager or Assistant Head of Service as prescribed by the Regulation of Investigatory Powers (Prescription of Offices, Ranks and Positions) (Scotland) Order 2000. (SI 2000:343) For the purposes of East Lothian Council the Investigations Manager will be no lower than fourth tier level and the Assistant Head of Service no lower than third tier level. For public authorities there are no substitutes of lower grade officers prescribed to authorise 'urgent' cases in contrast, for example, to the police.

6.2 Authorising officers within the meaning of this procedure should avoid authorising their own activities wherever possible and only do so in exceptional circumstances. An authorising officer can also act as a controller or handler of a source.

6.3 Authorisations will be in writing. However, in urgent cases a third tier level Manager or Head of Service or above may approve applications orally.

6.4 All applications for covert human intelligence source authorisations will be made on form ELC/AUTH/CHIS. The applicant in all cases should complete this. In urgent cases an oral authorisation may be given by the authorising officer. A statement that the authorising officer has expressly granted the authorisation should be recorded on the form or, if that is not possible, in the applicant's notebook or diary. This should be done by the person to whom the authorising officer spoke (normally the applicant) but should later be endorsed by the authorising officer.

6.5 All applications for covert human intelligence source renewals will be made on form **ELC/REN/CHIS.** The applicant in all cases should complete this where the source work requires to continue beyond the previously authorised period (including previous renewals).

6.6 Where authorisation ceases to be either necessary or appropriate the authorising officer or appropriate deputy will cancel an authorisation using form **ELC/CAN/CHIS**.

6.7 Forms, codes of practice and supplementary material will be available from the Council Intranet and those departments authorising action under The RIP(S)Act and the RIP Act and will be maintained by Trading Standards and Legal and Committee Services.

6.8 Any person giving an authorisation for the use or conduct of a source must be satisfied that:

Account has been taken of the likely degree of intrusion into the privacy of persons other than those directly implicated in the operation or investigation ('collateral intrusion'). Measures must be taken, wherever practicable, to avoid unnecessary intrusion into the lives of those affected by collateral intrusion.
The authorisation is necessary.
The authorised use or conduct is proportionate.
Satisfactory arrangements exist for the management of the source.

6.9 Authorisation for use of a Covert Human Intelligence Source can only be granted if sufficient arrangements are in place for handling the source's case. The arrangements that are considered necessary are that:

6.9.1 There will at all times be a person holding the requisite office, rank or position with the relevant investigating authority who will have day to day responsibility for dealing with the source on behalf of that authority and for the source's security and welfare – this should be the source's line manager (the Handler).

6.9.2 There will at all times be another person holding the requisite office, rank or position with the relevant investigating authority who will have general oversight of the use made of that source – this should be the handler's line manager (the Controller).

6.9.3 There will be at all times a person holding the requisite office, rank or position with the relevant investigating authority who will have responsibility for maintaining a record of the use made of that source – this should be the Authorising Officer

6.9.4 The record relating to the use of that source shall be maintained by East Lothian Council which will always contain particulars of such matters as may be specified in regulations made by the Scottish Ministers.

6.9.5 The records maintained by East Lothian Council that discloses the identity of the source will not be available to persons except to the extent that there is a need for access to them to be made available to those persons.

6.10 NECESSITY

Source work shall only be undertaken where there is no reasonable and effective alternative way of achieving the desired objective(s).

6.11 Effectiveness

Planned undercover operations shall be undertaken only by suitably trained or experienced employees, or under their direct supervision.

6.12 **Proportionality**

The use of covert human intelligence sources shall not be excessive i.e. it shall be in proportion to the significance of the matter being investigated.

6.13 **Authorisation**

All use and conduct of covert human intelligence sources shall be authorised in accordance with this procedure.

6.14 Additionally, the authorising officer must make an assessment of any risk to a source in carrying out the conduct in the proposed authorisation.

6.15 Use of a covert human intelligence source with technical equipment

6.15.1 A covert human intelligence source wearing or carrying a surveillance device and invited into residential premises or a private vehicle does not require special authorisation to record activity taking place inside the premises or vehicle. Authorisation for the use of that covert human intelligence source may be obtained in the usual way.

6.15.2 Applicants should apply within their own line management structure unless other arrangements have been agreed or it is unreasonable or impractical in the circumstances.

6.15.3 Services wishing to adopt a more devolved authorisation process may do so only on the explicit approval of a written policy by the Council; all authorisations must remain within the scope of the Scottish Executive's guidance on authorising grades.

7. Time Periods – Authorisations

7.1 Oral applications expire after 72 hours hours beginning with the time the authorisation was originally granted or renewed whichever is the later. If required they can be renewed for a further period of 12 months if renewed in writing.

7.2 Written authorisations expire 12 months after the day on which they took effect unless they are for Juvenile sources when the period of authorisation is one month.

8. TIME PERIODS – RENEWALS

8.1 If at any time before an authorisation would expire (including oral authorisations) the authorising officer considers it necessary for the authorisation to continue for the purpose for which it was given, it may be renewed in writing for a further period of 12 months beginning with the day on which the previous authorisation ceases to have effect. Applications should only be made shortly before the authorisation is due to expire.

8.2 Any person entitled to authorise may renew authorisations. They may be renewed more than once, provided they continue to meet the criteria for authorisation.

8.3 Authorisations for the deployment of a juvenile source are renewable for one further period of 1 month.

9. Review

9.1 The Authorising Officer shall review all authorisations at intervals of not more than one month. Details of the review and the decision reached shall be noted on the original application. More frequent reviews may take place at intervals to be determined by the Authorising Officer where the surveillance involves collateral intrusion or access to confidential information.

10. Cancellation

10.1 The authorising officer or appropriate deputy must cancel an authorisation if he/she is satisfied that the use or conduct of the source no longer satisfies the criteria for authorisation or that procedures for the management of the source are no longer in place. Where possible, the source must be informed that the authorisation has been cancelled.

Monitoring

11.1 Each Service or discrete location within Services must maintain a record of all applications for authorisation (including refusals), renewals, reviews and cancellations. The most senior authoriser in that Service or at that location will maintain the monitoring sheet form ELC/MS/RIPSA.

12. Security and Retention of Documents

12.1 Documents created under this procedure are highly confidential and shall be treated as such. Services shall make proper arrangements for their retention, security and destruction, in accordance with the requirements of the Data Protection Act 1998 and the Code of Practice.

12.2 The Head of Policy and Business Management will maintain the Central Register of Authorisations. Authorising officers shall notify the said Head of the grant, renewal or cancellation of any authorisations

and the name of the Applicant Officer within 24 hours to ensure the accuracy of the Central Register. Copies of the forms dealing with the grant, renewal or cancellation of any authorisations will be sent within the same period of time to the said Head.

12.3 The Authorising Officer shall retain the original Authorisation and Renewal forms until cancelled. On cancellation, the original Application, Renewal and Cancellation forms shall be forwarded to the Head of Policy and Business Management with the Authorising Officer retaining a copy.

12.4 The Authorising Officer shall retain the copy forms for at least one year after cancellation. The Head of Policy and Business Management will retain the original forms for at least three years after cancellation. In both cases these will not be destroyed without the authority of the authorising officer if practicable... Where the evidence from a surveillance operation is likely to be required for civil or criminal proceedings legal advice should be sought prior to any destruction.

12.5 All information recovered through the use of a source which is relevant to the investigation shall be retained for at least five years after the cancellation of the authorisation or the completion of any Court proceedings in which said information was used or referred to. All other information shall be destroyed as soon as the operation is cancelled.

13. Oversight

13.1 The Office of Surveillance Commissioners (OSC) provides independent oversight of the use of the powers contained within the Regulation of Investigatory Powers (Scotland) Act 2000. This oversight includes inspection visits by Inspectors appointed by the OSC.

14. Complaints

14.1 The Regulation of Investigatory Powers Act 2000 (the 'UK Act) establishes an independent Tribunal. This has full powers to investigate and decide any cases within its jurisdiction.