GLASGOW CITY COUNCIL POLICY AND GUIDELINES ON COVERT SURVEILLANCE AND HUMAN INTELLIGENCE SOURCES

This is the Policy and Guidelines on Covert Surveillance and Human Intelligence Sources as approved by the Policy and Resources Committee on 20 November 2001 and by Full Committee on 29 November 2001.

Part One : Policy Background

1.1 INTRODUCTION

In some circumstances, it may be necessary for Council employees, in the course of their duties, to make observations of a person(s) or premises in a covert manner, i.e. it is done so that those under observation are unaware that they are being observed. It may also be necessary to instruct third parties to do so on the Council's behalf. By their nature, actions of this sort are potentially intrusive (in the ordinary sense of the word) 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'). Similar considerations arise in relation to the use of undercover agents or informants who are referred to as "covert human intelligence sources".

The Regulation of Investigatory Powers (Scotland) Act (2000) ("RIPSA") provides, for the first time, a legal framework for covert surveillance by public authorities and an independent inspection regime to monitor these activities.

1.2 OBJECTIVE

The objective of this policy is to ensure that all covert surveillance carried out by or on behalf of the Council or any use of covert human intelligence sources is carried out effectively, while remaining in accordance with the law. It should be read in conjunction with the Scottish Executive's Code of Practice on Covert Surveillance ("the Code of Practice") and the Code of Practice on the Use of Covert Human Intelligence Sources ("the CHIS Code of Practice"). An edited version which reproduces parts of the Code of Practice of relevance to the Council is also available.

If the procedures outlined in this policy are not followed, any evidence acquired will have been acquired unlawfully. It may therefore not be admissible in court, and the Procurator Fiscal is unlikely to take proceedings on the basis of such evidence. The Council may also be exposed to legal action.

1.3 SCOPE OF THE POLICY

This Policy applies in all cases where "directed surveillance" is being planned or carried out. Part 4 of the Policy applies to the use of covert human intelligence sources. Directed Surveillance is defined in RIPSA as 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". "Private information" means information relating to a person's private or family life. If an operation is neither intended nor likely to obtain private information, then it will not be necessary to apply this policy. The Policy does not apply to activities undertaken by the Council as a result of information discovered through the use of surveillance.

The procedure does not apply to ad-hoc covert observations that do not involve the systematic surveillance of specific person(s). Equally, it does not apply to observations that are not carried out covertly, or to unplanned observations made as an immediate response to events. In cases of doubt, the authorisation procedures described below should however be followed.

1.4 COVERT HUMAN INTELLIGENCE SOURCES

The use of a "covert human intelligence source" (i.e. Council officers acting in an undercover capacity, or the use of informants) (hereafter referred to as "sources") raises similar issues to directed surveillance. The use of such sources is covered by Part 4 of this Policy, to which reference must be made. Council Officers making undisclosed site visits or test purchases do not count as "covert human intelligence sources" and such activities do not require formal authorisation. Some operations may involve both the use of a source and directed surveillance, in which case both aspects require to be authorised.

1.5 PRINCIPLES OF SURVEILLANCE

In planning and carrying out covert surveillance, officers of Glasgow City Council shall comply with the following principles:

Lawful purposes – covert surveillance shall only be carried out where necessary to achieve one or more of the permitted purposes (as defined in RIPSA); i.e. it must be :

(a) for the purpose of preventing or detecting crime or the prevention of disorder;

(b) in the interests of public safety; or

(c) for the purpose of protecting public health.

Employees carrying our surveillance shall not cause damage to any property or harass any person in the course of conducting the surveillance.

Necessity – covert surveillance shall only be undertaken where there is no reasonable and effective alternative way of achieving the desired objective(s).

Proportionality – the use and extent of covert surveillance shall not be excessive i.e. it shall be in proportion to the significance of the matter being investigated.

Intrusive surveillance – no activity shall be undertaken that comes within the definition of "intrusive surveillance", i.e. if it involves surveillance of anything taking place within residential premises or in a private vehicle.

Collateral intrusion – reasonable steps shall be taken to minimise the acquisition of information that is not directly necessary for the purposes of the investigation or operation being carried out.

Authorisation – all directed surveillance **must** be authorised in accordance with the procedures described below.

Part Two : Seeking Authorisation

2.1 WHEN IS AUTHORISATION REQUIRED?

Authorisation is required for "directed surveillance" i.e. surveillance which is "covert" but not "intrusive". This means surveillance for the purposes of a specific investigation or operation, whether or not the identity of those who will be observed by the surveillance is known in advance. The surveillance must be undertaken in a manner likely to acquire "private information" about a person or persons (which is not defined but includes information about their private and family life). It must be conducted in such a manner as is calculated to ensure the persons subject to the surveillance are unaware that it is or may be taking place. Thus overt CCTV systems (where the cameras are plainly visible and signs advising of the presence are displayed) is not caught; however placing a hidden camera to discover who is pilfering supplies is. The surveillance must take place otherwise than by way of an immediate response to events or circumstances the nature of which is that it would be impractical to seek authorisation before carrying out the surveillance. Authorisation is required whether the activity is done by Council officers themselves or by third parties carrying out surveillance on behalf of and under the instructions of the Council (such as private investigators or the neighbours of anti-social tenants).

2.2 WHO MAY SEEK AUTHORISATION?

Any officer whose duties involve activity falling within the above description may seek authorisation to do so and must seek and be granted authorisation prior to carrying out the surveillance. This is most likely to arise in services responsible for policing, enforcement or security functions. A standard application form for directed surveillance authorisation is appended to this Policy.

2.3 INTRUSIVE SURVEILLANCE

Intrusive surveillance means surveillance in relation to anything taking place within any residential premises (i.e. a person's accommodation, however temporarily used, but not common areas such as common stairs and closes) or in any private vehicle. The Council is not authorised to conduct intrusive surveillance under any circumstances.

Some additional points should be made about intrusive surveillance. Firstly surveillance is not intrusive if directed into a home or private vehicle from outside unless the information is consistently of the same quality as the device actually present in the home or vehicle would provide. Advice from the Office of Surveillance Commissioners (OSC) suggests that the sort of surveillance undertaken by the Council is unlikely to reach this level of sophistication. Thus activities such as filming goods being sold from the back of a car, or monitoring the level of noise generated by an anti-social tenant (but not the actual words) are unlikely to be classed as intrusive, and so these activities can safely be carried out (subject to appropriate authorisation).

Secondly, devices carried into a home or private vehicle by a covert human intelligence source do not constitute intrusive surveillance so long as the source has been invited in. However the device must not be left behind when the source leaves the premises or vehicle. Services are reminded of the need to have proper authorisation under Section 4 of this Policy before any use is made of a source.

2.4 WHEN IS COVERT SURVEILLANCE APPROPRIATE?

By its nature covert surveillance intrudes on people's privacy. It should therefore be regarded as a final option, only to be considered when all other methods have either been tried and failed, or where the nature of the activity the surveillance relates to is such that it can reasonably be concluded that nothing else will be able to acquire the

information being sought. Thus, for example, if a vending machine is regularly broken into consideration should be given to installing overt CCTV cameras (with appropriate signage) before installing hidden cameras.

Any use of covert surveillance must be proportionate to the objective being pursued.

2.5 PROPORTIONALITY

Proportionality is a concept of human rights law designed to ensure that measures taken by the State (and its organs such as the Council) which impact on the rights of citizens are kept within proper bounds. It means that if the same legitimate end can be reached by means of less intrusion on people's rights (or none at all) then the less intrusive path should be taken. There should also be a reasonable relationship between the seriousness of the mischief being addressed and the degree of intrusion into people's rights.

Covert surveillance involves a potentially serious breach of individuals' right to privacy. Compelling reasons are therefore required to justify these, particularly if the surveillance is to continue for an extended period. Thus surveillance of a staff member on sick leave is likely to be disproportionate if all that is being assessed is a possibly fraudulent claim for a very small amount of statutory sick pay, but it may be proportionate in detecting a fraudulent legal claim against the Council for thousands of pounds.

It is useful to consider how serious the breach you are seeking to rectify is. For criminal offences the potential sentence may be a useful guide. However many regulatory offences, while attracting only very small fines, are designed to prevent potentially life threatening occurrences (such as sale of dangerous goods or contaminated food, or the overcrowding of licensed premises). Such factors weigh in favour of surveillance being proportionate. Another factor to consider is the impact of the breach on other people, both in terms of seriousness of the offences and the numbers affected.

2.6 CONFIDENTIAL MATERIAL AND COLLATERAL INTRUSION

Confidential material covers a number of areas: professional legal advice given to someone, health information, spiritual counselling, and material held under an obligation of confidentiality (particularly if held for the purposes of journalism). So far as possible surveillance operations should be designed so as to minimise or eliminate the possibility of confidential information being acquired. If confidential information is in fact acquired, special care should be taken to avoid unnecessary disclosure of it.

"Collateral Intrusion" refers to the fact that very often surveillance operations will inadvertently intrude on the privacy of persons other than those at whom the operation is directed. Operations should be planned so as to minimise or eliminate so far as possible the risk of collateral intrusion, and the extent to which it remains is a factor to consider in determining the proportionality of the operation.

2.7 SURVEILLANCE BY OTHER PUBLIC AUTHORITIES

Council officers are occasionally asked to assist in surveillance operations being conducted by other public authorities such as the Police, the Benefits Agency, Customs and Excise etc. In such cases it is for the organisation seeking assistance from the Council to ensure that it has appropriate authorisations in place. These authorisations should be shown to the Council staff involved or else written confirmation be given that the authorisations have been duly granted. If the Council is carrying out its own surveillance as part of a joint operation however it will be appropriate for the Council to put its own authorisations in place too. Protocols regulating such assistance and joint operations have been or are being put in place. Reference should be made to these where appropriate.

Part Three : Granting and Recording Authorisations and Refusals

3.1 WHO MAY GRANT AUTHORISATIONS?

In terms of the Regulations, authorisations for directive surveillance may only be granted by the Head of Service i.e. the Chief Executive, Assistant Head of Service i.e. the Solicitor to the Council or an Investigation Manager. Investigation Managers for the Council have been designated through an amendment to the Scheme of Delegated Functions. Previously, the Chief Executive authorised a number of senior officers to act as Investigation Managers as an interim measure, and may do so for operational reasons in the future. The line managers of any designated Investigation Manager may also grant authorisations.

In the absence of the Director or other designated Investigation Manager, Services should seek authorisation from the Solicitor to the Council. If a number of authorisations are likely to be required however the relevant Director should approach the Chief Executive in order to have additional departmental Investigation Managers designated. In general an Investigation Manager should be a third tier officer or above. Good practice dictates that the officer authorising surveillance is not operationally involved in the matter being authorised, although this may not always be practicable.

3.2 RECEIPT AND LOGGING OF APPLICATIONS

All services carrying out surveillance activities must maintain a record of all applications for direct surveillance, together with the relevant consent for refusal. These forms may be monitored for cross-service consistency by the Chief Executive, and may have to be produced in the event of an inspection by the OSC. These forms represent evidence of the Council's compliance with the law and Code of Practice, and as such care should be taken in the completion and logging of them. All Services undertaking surveillance (including making applications for authorisation which are refused) must notify the Chief Executive in writing of the arrangements made locally for the storage of authorisations and refusals.

3.3 CENTRAL REGISTER OF AUTHORISATIONS AND REFUSALS

All services undertaking surveillance activity must, at the end of each calendar month, notify the Chief Executive in writing of:

- Any new authorisations granted that month;
- Any application which have been refused; and
- Any authorisations granted previously which still subsist.

The Chief Executive shall maintain a confidential central register of such authorisations and refusals.

3.4 GRANT OR REFUSAL OF AUTHORISATIONS

The OSC may require an Authorising Officer to justify their decision to grant a request, so authorisations should not be signed off automatically. Evidence of reasoned refusal of requests is also vital in displaying compliance with the law. If evidence is obtained by surveillance is used in court, it will be the authorising officer who will be called on to justify the grant of the authorisations.

The Authorising Officer's job is to be satisfied that the Applicant Officer has correctly identified a lawful purpose for the proposed surveillance, has planned the operation properly so as to minimise collateral intrusion and the collection of confidential information, is not proposing to stray beyond the permissible bounds of directed surveillance, and has correctly applied the proportionality test. Only if actively satisfied on these points should the authorisation be granted. Any restrictions imposed on the authorisation should be noted as Authorising Officer comments.

3.5 DURATION, RENEWAL AND CANCELLATION OF AUTHORISATIONS

By law an authorisation lasts for three months. However for Council purposes it is suggested that authorisations generally should only be granted on the presumption that they will be cancelled after one week. Continuous surveillance which has failed to uncover evidence within one week is a questionable use of resources, quite apart from the fact that long term surveillance is harder to justify in terms of proportionality. Longer periods of occasional surveillance may, however, be required to establish e.g. a pattern of behaviour or activity. If the reasons justifying carrying out the surveillance cease to apply, then the authorisation must be cancelled and a record kept of the cancellation and the reasons for this. However, if the surveillance is non-intrusive (e.g. if it involves periodic inspection rather than continuous monitoring) then it may be appropriate to adopt a two-weekly review. This would also apply if the surveillance is conditional on other factors (e.g. it will require officers to work overtime and the overtime has not yet been approved).

If surveillance is to be continued for longer than three months, it is necessary to have a renewal authorised. Renewal applications should highlight the fact that what is sought is a renewal, and enclose the original authorisation and any previous renewals. The tests applicable to renewals are identical to those for initial applications.

There should be a weekly or fortnightly review of all authorisations granted by the Authorising Officer or, in his or her absence, by their line manager. This review should note whether any significant evidence has been acquired by the activity being considered and whether, against that background, continued surveillance can still be justified. Reviews should be noted on the authorisation. As soon as a review indicates that surveillance can no longer be justified, the authorisation must be cancelled. It is not good practice to allow authorisations to continue to run once they have served their usefulness. If it is apparent at any stage that authorisation is no longer required, it should be cancelled immediately and not left to the next review. The Authorising Officer must advise the officers conducting surveillance that the authorisation has been cancelled. The date and time when this is done must be recorded on the authorisation form.

3.6 SECURITY AND RETENTION OF DOCUMENTS

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. It should be noted that refusals as well as approved applications must be retained. The Code of Practice recommends retention of authorisations for five years (longer if required for ongoing proceedings). Services must also make appropriate arrangements to ensure the security of the evidence acquired, which is likely to be of a sensitive nature

In accordance with the recommendations of the Office of Surveillance Commissioners ("OSC"), documents will be inspected periodically by the Chief Executive or his representative to ensure that a consistent approach is being adopted by different Council services. The OSC have statutory powers of inspection and all records (applications, authorisations, refusals) must be available for inspection. No records should be destroyed until after an OSC inspection has had the opportunity to see them.

Each Service carrying out surveillance activities must make appropriate arrangements for the secure storage of authorisations and refusals. As stated above, the Chief Executive should be advised of these arrangements.

3.7 DATA PROTECTION ACT 1998:

Surveillance "product" (i.e. the evidence acquired) will, in almost all cases, constitute "personal data" and so be covered by the provisions of the Data Protection Act 1998. This Act requires that personal data should (amongst other things) be adequate, relevant, accurate, up-to-date, not excessive, and must be kept secure. Surveillance planning and retention arrangements should be designed around these issues.

In relation to the relevance of personal data, the Code of Practice advises that material acquired as a result of "collateral intrusion" should be removed from files. In applying this principle, however, services must be extremely alert to the risk of endangering the evidential value of the material to be retained.

In accordance with the normal rules, data subjects enjoy wide (but not unlimited) rights of access to the data held on them. Requests for access to material acquired by surveillance should be treated in the usual way i.e. forwarded immediately to the Data Protection Officer (Internal Audit, 108 Ingram Street). Access will, in many cases, be denied on the grounds of possible prejudice to the prosecution of offenders, but this decision must be reached on a case by case basis.

Part Four : Covert Human Intelligence Sources

4.1 SCOPE OF THIS PART

This part of the Policy regulates the use of covert human intelligence sources, or "sources" for short. It must be read alongside the CHIS Code of Practice. Use of a source specifically includes inducing, asking or assisting a person to act as a source. Accordingly the procedures laid out in this Part should be followed **before** any outside party is approached with a view to having them act as a source.

4.2 WHAT IS A COVERT HUMAN INTELLIGENCE SOURCE?

In terms of RIPSA, a source is a person who establishes or maintains a personal or other relationship with another person and who either uses that relationship covertly to obtain information or who covertly discloses information obtained through the relationship or obtained as a consequence of its existence. The main concern generated by this is that the source effectively exploits the relationship as a means of covertly acquiring information. This should be distinguished from activities where there is no such exploitation. Thus an unannounced site visit by Council officers for the making of test purchases do not involve the exploitation of a relationship and so will not fall to be classified as covert source activity. Similarly asking a concerned citizen to "keep an eye" on suspicious behaviour will not (by itself) amount to source activity, although it may amount to surveillance conducted on behalf of the Council.

4.3 WHEN IS IT APPROPRIATE TO USE A SOURCE?

The covert exploitation of a relationship is arguably a greater interference with personal privacy than covert surveillance. The deployment of a source may also expose the source himself or herself to serious danger. For these reasons the use of covert human intelligence is to be discouraged and should only be used by the Council as an absolute last resort. Activity, the nature of which would justify the use of a covert source will in the majority of cases be more appropriately dealt with by the Police. In all cases where the use of a covert source is being considered, a full risk assessment must be undertaken with a view to evaluating whether the evidence being sought (and the use it will be put to) justify exposing the source to the risks involved. Operational planning should be built around the safety and security of the source.

4.4 WHEN CAN THE USE OF A SOURCE BE AUTHORISED?

The use of a source is only lawful in the circumstances described in paragraph 1.5. In evaluating these criteria it is important to note that in terms of proportionality (see also paragraph 2.5) more will be required to justify the use of a covert source than would be required to justify the use of directed surveillance.

4.5 AUTHORISATION PROCESS

The authorisation process for covert source use is similar to that for directed surveillance. An application must be made in writing to a designated investigation manager. While all investigations managers are permitted in law to authorise the use of a covert source, for purposes of this Policy authorisations may only be granted by directors (or in their absence by depute directors), the Chief Executive, Solicitor to the Council and Head of Internal Audit. Applications must be made on the form attached to this Policy.

4.6 HANDLERS AND CONTROLLERS.

It is a legal pre-requisite to the use of a covert source that proper arrangements have been put in place for handling the source's case. RIPSA requires two officers to be designated for this purpose: the "handler" who has day to day responsibility for dealing with the source on behalf of the Council, and for dealing with the source's security and welfare. Secondly there must be a "controller" who has general oversight of the use made of the source. In terms of this Policy the controller must be more senior in post than the handler. All applications for covert source authorisation must indicate who the proposed handler and controller are. Both handler and controller must agree to be so designated and indicate their willingness to perform their respective duties. Only the handler, controller and authorising officer will know the identity of the source, whose identity should be carefully protected.

4.7 SOURCE RECORDS

RIPSA requires that there be a person having specific responsibility for maintaining a record of the use of a source. In terms of this Policy this responsibility lies with the authorising officer. By law any records which disclose the identity of the source must only be made available to those having a need to access them. Services making use of covert sources must inform the Chief Executive of the arrangements being made for the security of such records. The requirements for record keeping and central notification of authorisations in Part 3 apply equally to authorisations, renewals and cancellations made under this Part 4. The Chief Executive should not normally be advised as to the identity of the source.

Part Five – Complaints And Review

5.1 COMPLAINTS

Anyone who wishes to complain about surveillance which they believe the Council is carrying out or any use by the Council of a CHIS should write, in the first instance, to the Director of the Service which is thought to be conducted the surveillance. If this is not known, the complaint should be addressed to the Chief Executive.

On receiving a complaint, the Council will appoint an officer not involved in the operation to check whether what has been done (if, indeed, anything is being done) complies with to the terms of the law, Code of Practice, and this policy. However, it will often be the case that the Council is unable to confirm or deny whether surveillance has been taking place, or whether someone is operating as a CHIS, as such information may in itself prejudice the Council's regulatory functions or endanger the source. The outcome of such an internal review may therefore fail to satisfy a complainant.

5.2 EXTERNAL REVIEW

The legislation sets up a system whereby complaints about surveillance (or alleged surveillance) or the use/alleged use of a covert human intelligence source can be made to an independent body, the Investigatory Powers Tribunal. Anyone making a complaint to the Council should be advised of this option. Complaints should be made in writing to:

The Investigatory Powers Tribunal
PO Box 33220
London SW1H 9ZQ

Explanatory leaflets, complaint forms, copies of the Code of Practice and this Policy should be available at public offices of services conducting surveillance.

GLASGOW CITY COUNCIL

REGULATION OF INVESTIGATORY POWERS (SCOTLAND) ACT 2000

APPLICATION FOR AUTHORITY FOR DIRECTED SURVEILLANCE

Name of Applicant		**Department / Section**	
Full Address			
Contact Details			
Operation Name / File reference:		For renewals of existing authorisations only: number of previous authorisations.	

Details of application: **(For renewals, please attach all previous authorisations).**

1. Grounds on which the action is <u>necessary</u>: *(Tick as applicable):*	
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	☐

2. Explain why the directed surveillance is proportionate to what it seeks to achieve

3. The identities, where known, of those to be subject of the directed surveillance:

Name:

Address:

DOB:

Other information as appropriate:

4. The action to be authorised, including any premises or vehicles involved;

5. Give an account of the investigation or operation:

6. Explanation of the information which it is desired to obtain as a result of the authorisation:

7. Collateral intrusion:

INDICATE ANY POTENTIAL FOR COLLATERAL INTRUSION ON OTHER PERSONS THAN THOSE TARGETED: INCLUDE A PLAN TO MINIMISE COLLATERAL INTRUSION

8. Confidential / Religious Material:
INDICATE THE LIKELIHOOD OF ACQUIRING ANY CONFIDENTIAL / RELIGIOUS MATERIAL:

Anticipated Start	**Date:**	**Time:**

9. Authorising Officer's Comments.

10. Authorising Officer's Recommendation.
I, _____[insert name], hereby authorise the directed surveillance operation as detailed above. This written authorisation will cease to have effect at the end of three months unless cancelled earlier or renewed: The continuing validity of this authorisation shall be subject to review by me, the authorising officer, at the following intervals: One week (recommended) ☐ Two weeks ☐ Other (specify: _____) . ☐ Reason for extended review period of greater than two weeks:

Name (Print)		**Post**	
Signature		**Date**	

11. Review (to be completed by Authorising Officer)**.**		
Date	**Details**	**Signature**

12. Cancellation	
Date and Time of Cancellation	**Comments**
Date and Time Surveillance Officers Notified	
A/O's Signature	

GLASGOW CITY COUNCIL

REGULATION OF INVESTIGATORY POWERS (SCOTLAND) ACT 2000

APPLICATION FOR AUTHORITY FOR THE USE OR CONDUCT OF A COVERT HUMAN INTELLIGENCE SOURCE

Name of Applicant		**Department / Section**	
Full Address			
Contact Details			
Proposed Handler (Name and Post)		**Proposed Controller (Name and Post)**	
Operation Name / File reference:		For renewals of existing authorisations only: number of previous authorisations.	

Details of application: **(For renewals, please attach all previous authorisations).**

1. Grounds on which the action is <u>necessary</u>: *(Tick as applicable):*	
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	☐

2. Explain why the authorised conduct or use of a source is proportionate to what it seeks to achieve

3. Summary of the risk assessment conducted in relation to this proposal (The full risk assessment must be attached).

4. Details of the purpose for which the source will be tasked or deployed (i.e. nature of the conduct which the source will assist in addressing):

5. Give an account of the investigation or operation:

6. Details of what the source will be tasked to do:

7. Collateral intrusion:

INDICATE ANY POTENTIAL FOR COLLATERAL INTRUSION ON OTHER PERSONS THAN THOSE TARGETED: INCLUDE A PLAN TO MINIMISE COLLATERAL INTRUSION

8. Confidential / Religious Material:
INDICATE THE LIKELIHOOD OF ACQUIRING ANY CONFIDENTIAL / RELIGIOUS MATERIAL:

Anticipated Start	**Date:**	**Time:**

9. Authorising Officer's Comments. (A/O must be a Depute Director or above).

10. Authorising Officer's Recommendation.

I, _____[insert name], hereby authorise the conduct or use of a covert source as detailed above. This written authorisation will cease to have effect at the end of) twelve months unless cancelled earlier or renewed:

The continuing validity of this authorisation shall be subject to review by me, the authorising officer, at the following intervals:

One week (recommended) ☐

Two weeks ☐

Other (specify: _____) . ☐

Reason for extended review period of greater than two weeks:

Name (Print)		**Post**	
Signature		**Date**	

11. Review (to be completed by Authorising Officer)**.**		
Date	**Details**	**Signature**

12. Cancellation	
Date and Time of Cancellation	**Comments**
Date and Time Controller and Handler Notified	
Date and Time Source Notified	
A/O's Signature	