APPENDIX 1

ANGUS COUNCIL

THE REGULATION OF INVESTIGATORY POWERS (SCOTLAND) ACT 2000 ("RIP(S)A")

POLICY AND GUIDELINES ON THE USE OF COVERT SURVEILLANCE AND COVERT HUMAN INTELLIGENCE SOURCES

Version:	V01
Author:	David Thompson
Owner:	Jackie Buchanan
Date of Approval:	27 October 2020
Approved by:	P & R Committee
Date issued:	27 October 2020
Review Period	Annually
Review Date	October 2022
Next review date:	October 2023

Amendment Form

Version	Date	Brief Summary of Changes	Author

1. POLICY BACKGROUND

1.1 Introduction

This policy and related documents were initially approved by the Policy and Resources Committee of Angus Council on 4 December 2001. It has subsequently been updated in line with the Scottish Government's Codes of Practice, which came into force on 11 March 2003 and recommendations received from the Office of Surveillance Commissioners (OSC). The amended policy was approved by the Strategic Policy Committee of the council at its meeting on 16 March 2004 (Report No 362/04 refers). It has been, and will continue to be, further refined in line with arising developments, such as new case law or further recommendations from the Investigatory Powers Commissioner's Office (IPCO) (the successors of the OSC since 2017).

This Policy and Guidelines will be reviewed annually, and any changes reported to the Policy and Resources Committee.

Angus Council is a public authority for the purposes of RIP(S)A and has the power to authorise directed covert surveillance and the use of covert human intelligence sources. Covert activities covered by RIP(S)A will be lawful if the activities are authorised and if they are conducted in accordance with the authorisation.

In some circumstances, it will be necessary for council employees, in the course of their duties, to make observations of a person in a covert manner, i.e. without that person's knowledge, or to instruct third parties to make such observations on the council's behalf. By their very nature, actions of this sort are potentially intrusive (in the ordinary sense of the word) and may be legally challenged as breaching Article 6 (right to a fair trial), Article 8 (the right to respect for private and family life) and to a lesser extent Article 1 of Protocol 1 (the right to respect for property) of the European Convention on Human Rights (ECHR).

RIP(S)A provides, for the first time, a legal framework for the carrying out of covert surveillance by public authorities and an independent inspection regime to monitor these activities.

The Chief Executive is the RIP(S)A Senior Authorising Officer (SAO), who has oversight and scrutiny in relation to the RIP(S)A and ensures the integrity of the processes in place and acts as the main point of contact with the Investigatory Powers Commission. In the Chief Executive's absence, the Director of Legal and Democratic Services will deputise.

The council's Senior Responsible Officer is the Director of Legal and Democratic Services.

There are a number of Authorised Officers across the council who are appointed by the Chief Executive.

1.2 Objective

The objective of this policy is to ensure that all covert surveillance carried out by or on behalf of council departments is carried out effectively and lawfully. It should be read in conjunction with the Scottish Government's Code of Practice on Covert Surveillance and Code of Practice on the Use of Covert Human Intelligence Sources, the Communication Data ("the Codes of Practice") and the OSC Procedures and Guidance on Covert Surveillance and Property Interference. All of these are available on the Council's RIP(S)A intranet page.

If the procedures outlined in this policy are not followed, the evidence acquired as a result of the covert surveillance may have been acquired unlawfully. Such evidence 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 for breaching the ECHR and may be the subject of a complaint to the tribunal set up by the UK wide Regulation of Investigatory Powers Act 2000.

1.3 Seeking further Advice

Although this guidance is designed to assist day-to-day application of RIP(S)A, it will sometimes be essential to seek further advice, including legal advice, on difficult cases. The council's contact for legal advice is the Information Governance Team within Legal and Democratic Services (InformationGovernance@angus.gov.uk).

1.4 Scope of the Policy

This policy applies in all cases where directed surveillance or the use of a covert human intelligence source (CHIS) 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 which is likely to result in the obtaining of private information about a person (this and other terms are defined in the glossary in Part A of Appendix One). It may be noted that the courts have determined in the context of European Convention of Human Rights jurisprudence that the term "private life" merits a wide interpretation and this will include professional and business activities. If in doubt, therefore, it is always safer to presume the requirement for a RIP(S)A authorisation.

A CHIS is someone who establishes or maintains a relationship with another person with the intention of covertly obtaining information from that person.

Any authorisation sought or carried out in terms of this policy must be done in accordance with the principles of surveillance set out in the Codes of Practice and reproduced at Part B of Appendix One.

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 observations that are not carried out covertly or to unplanned observations made as an immediate response to events.

However, in cases of doubt, the authorisation procedures described below should always be followed.

1.5 Covert Human Intelligence Sources (CHIS) - Special Procedures

The use of a CHIS (i.e. council officers acting in an undercover capacity or the use of informants) raises similar issues to directed surveillance. The principles in this policy are equally applicable to such undercover operations, which must meet the same tests as directed surveillance and be properly authorised.

However, additional rules apply to the use of a CHIS. These rules are set out in the Regulation of Investigatory Powers (Source Records) (Scotland) Regulations 2002 (SSI 2002/205). In addition, the CHIS Code of Practice sets out further records on sources to be kept by the council. These source record requirements are reproduced as Appendix Three to this guidance. These records do not form part of the central record of authorisations kept by the council and departments must make their own internal arrangements to ensure that these CHIS records are securely maintained.

In every CHIS case, there is a need to appoint a “handler” and a “controller” to be responsible for the security of the CHIS.

Because of these specialities, the relative risk and the relative infrequency of use of CHIS’s by Angus Council, it is policy that any service considering such activities should first consult The Information Governance Team within Legal and Democratic on what is required.

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.

2. 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.

Authorisation is required if:

- the surveillance is undertaken in a manner which is likely to acquire private information about one or more people ('private information' is not defined but includes information about a person's private and family life).

- the surveillance is to be conducted in such a manner as is calculated to ensure that the persons subject to the surveillance are unaware that it is or may be taking place. As a result, the use of overt CCTV systems (where the cameras are plainly visible and signs advising of the presence of the cameras are displayed) does not require authorisation under the Act, but placing a hidden camera to discover who is, e.g. stealing from a vending machine does.

- the surveillance takes place otherwise than by way of an immediate response to events, the nature of which is that it would be impractical to seek authorisation before carrying out the surveillance. (See 2.2 below).

- whether the activity is carried out by council officers themselves or by third parties carrying out directed surveillance on behalf of and under the instructions of the council (such as private investigators or the neighbours of anti-social tenants).

2.2 All covert activities which come within the scope of RIP(S)A must have written authority, except in an immediate response to circumstances that amount to covert conduct. Although, strictly, the necessity and proportionality tests do not apply to the "immediate response" situation (because authorisation is not required), council policy is that the officer concerned should still consider whether the "immediate response" surveillance is necessary and proportionate and note it as such. Such activities should not exceed one day. In any case, authorisation should be sought at the first possible opportunity. This all relates to "immediate response" surveillance. It is not possible to define that term but an example might be a trading standards officer coming across a counterfeit DVD seller at a car boot sale on a Sunday and deciding **there and then** to tail the seller in the expectation of discovering the whereabouts of the supplier.

Separate from the question of immediate response, it is also possible to obtain oral authorisation in cases of urgency.

Where it is impossible to obtain written authorisation, oral authorisations may be sought. Where this happens, an Authorising Officer must complete an application form on behalf of the requesting officer as fully as possible in order to justify the oral authorisation although in these situations consent may, where necessary, be obtained from a person who has not been appointed as an Authorising Officer. Oral authorisation should not exceed 72 hours and full written authorisation should be obtained at the first possible opportunity.

2.3 Who May Seek Authorisation?

Any suitably trained officer whose duties involve a surveillance activity falling within the description of directed surveillance contained in 2.1 may seek authorisation to do so and must seek and be granted authorisation (subject to the circumstances narrated in 2.2 above) **prior to** carrying out the surveillance. This is most likely to arise in departments responsible for regulatory, enforcement or security functions. Standard application forms for directed surveillance authorisation and for the use of covert human intelligence sources are available on the council's RIP(S)A intranet page (see Appendix Two for a list of the approved forms).

2.4 Intrusive Surveillance

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

Some additional points should be made about devices and intrusive surveillance. Firstly, surveillance is not intrusive if the device is directed into a home or private vehicle from outside of that home or vehicle unless the information provided from the surveillance is consistently of the same quality as would be provided by having a device actually present in the home or vehicle.
Advice suggests that the sort of surveillance undertaken by local authorities is unlikely to reach this level of sophistication. As a result, activities such as filming goods being sold from the back of a car or monitoring the level of noise generated by an antisocial tenant (but not the actual words spoken by the tenant) are unlikely to be classed as intrusive, and so these activities can be safely carried out by the council, subject of course to appropriate authorisation.

Secondly, devices carried into a home or private vehicle by a covert human intelligence source do not constitute intrusive surveillance provided that the CHIS has been invited in (or, indeed, invites him/herself in). However, the device must not be left behind when the CHIS leaves the premises or vehicle. Departments are reminded of the need to have proper authorisation (and the need to satisfy other requirements) before any use is made of a CHIS.

2.5 When is Covert Surveillance Appropriate?

Covert surveillance must first and foremost be for a lawful purpose. By its very 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 is reasonable to conclude that covert surveillance is the only way to acquire the information being sought. Using the earlier example, if a vending machine is regularly broken into, consideration should be given to installing overt CCTV cameras (with appropriate signage in terms of the Data Protection Act 2018) rather than installing hidden cameras.

2.6 Necessity

“Necessity” simply means that there is no other means by which the information could reasonably be obtained other than the covert means proposed. Therefore, alternative means of obtaining the information must always be considered.

2.7 Proportionality

“Proportionality” is a concept of Human Rights Law designed to ensure that measures taken by the state (and organs of the state 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 less intrusive means, 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 lives.

Covert surveillance involves a potentially serious breach of individuals' rights to privacy under Article 8 of the ECHR. Compelling reasons are therefore required to justify using covert surveillance, particularly if the surveillance is to continue for an extended period. 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.

In deciding whether any planned surveillance is proportionate, it is useful to consider how serious the breach you are seeking to rectify is. For criminal offences, the potential punishment by the Court (e.g. the maximum level of fine or length of prison sentence) may be a useful guide. However, many regulatory offences attract only very small fines, but are designed to prevent potentially life threatening situations (such as the sale of dangerous goods or contaminated food, or the overcrowding of licensed premises). Such factors weigh in favour of surveillance being proportionate.

When completing the requisite application forms a potential model answer would make clear that the four elements of proportionality had been fully considered:

- balancing the size and scope of the operation against the gravity and extent of the perceived mischief;

- explaining how and why the methods to be adopted will cause the least possible intrusion on the target and others;

- that the activity is an appropriate use of the legislation and the only reasonable way, having considered all others, of obtaining the necessary result; and

- providing evidence of other methods considered and why they were not implemented.

2.8 Collateral Intrusion

"Collateral Intrusion" refers to the fact that often surveillance operations will inadvertently intrude on the privacy of persons other than those at whom the operation is directed. It is part of the proportionality test. Operations should be planned so as to minimise or eliminate so far as possible the risk of collateral intrusion. When it is likely that the surveillance will intrude on other people's privacy, this will be a factor to consider in determining the proportionality of the operation.

2.9 Confidential Material

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 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 (reference should be made to the council's Data Protection Policy)

2.10 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,

Revenue and Customs 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 staff should receive written confirmation from the other authority 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 necessary for the council to put its own authorisations in place too.

2.11 Surveillance through Social Media

The internet may be used as a surveillance tool, and where online research or investigation is conducted covertly for the purpose of a specific investigation or operation and is likely to result in the obtaining of private information about a person or group, an authorisation for directed surveillance should be considered. Public use of the internet has expanded rapidly so that far more activity and interaction now occurs online than ever before. There may be a reduced expectation of privacy for material accessible on the internet, but privacy considerations may still apply, for example to information posted on social networking sites where the information may include or constitute private information. This is regardless of whether or not the account holder has applied any privacy settings to the account. Simple reconnaissance of such sites (i.e. preliminary examination with a view to establishing whether the site or its contents are of interest) is unlikely to interfere with a person's reasonably held expectation of privacy and therefore is not likely to require a directed surveillance authorisation. But where a public authority is systematically collecting and storing information about a particular person or group, a directed surveillance authorisation should be considered. A separate, detailed Surveillance through Social Media Policy has been developed and is available on the Council's RIP(S)A intranet page.

2.12 SITUATIONS WHERE THE REQUIREMENTS OF RIP(S)A CANNOT BE MET

There may be situations where covert surveillance is desired but the requirements of RIPSA cannot be met. In these cases, legal advice **MUST** always be sought prior to any action being taken, as an assessment of the nature of the issue, need for covert surveillance, risks/ mitigations associated with undertaking surveillance and privacy implications need to be addressed. In BA and others v Chief Constable of Cleveland Police, Cleveland Police (CP)(IPT/11/129/CH; IPT/11/133/CH & IPT/12/72/CH) placed a covert camera in a resident's flat to capture evidence that the resident's carers were stealing items from her. The authorisation of the use of such a camera did not fall within the definition of "intrusive surveillance" as the crime alleged was not "serious". Instead, CP undertook a similar approach to assess the privacy implications, risks, and mitigations of using a covert camera and authorised the conduct, albeit not under RIPA. Because there was proper consideration of whether an authorisation should be sought and this was evident, the Tribunal was satisfied that although the conduct was not protected by a surveillance authorisation, there was no unlawful activity or a breach of Article 8 of the Human Rights Act 1998.

3. GRANTING AND RECORDING AUTHORISATIONS AND REFUSAL

3.1 The statutory purposes for which covert surveillance authorisations may be issued must reflect the functions of the Council.

3.2 Who May Grant Authorisations?

Only Authorising Officers may grant authorisations for directed surveillance. In terms of Regulations made under RIP(S)A, only Service Leaders or their senior officers may be appointed as authorising officers. The Chief Executive has designated the holders of a number of posts in Angus Council as Authorising Officers. The Line Managers of any designated Authorising Officers may also grant authorisations. The Chief Executive or in her absence any Director of Angus Council who is an Authorising Officer must authorise any surveillance requests which may result in the gathering of confidential material or under circumstances covered by the Regulation of Investigatory Powers (Juveniles) (Scotland) Order 2002 (i.e. use of juvenile/vulnerable CHIS).

The Chief Executive also has the role and responsibility as Senior Authorising Officer (SAO) for authorisations which required a higher level of authorisation in cases where legally privileged information was likely to be acquired.

The Director of Legal & Democratic has the role and responsibilities as Senior Responsible Officer.

The Service Leader - Legal has the role of Gatekeeper for RIP(S)A matters who deals with completed RIP(S)A applications, reviewing and cancellation forms. The Gatekeeper also holds the Central Record of Authorisations.

The officer authorising surveillance shall generally not be operationally involved in the surveillance being authorised. As a result, departments should ensure that a sufficient number of members of staff have been appointed and trained as Authorising Officers.

Departments without a designated Authorising Officer should seek authorisation from the Chief Executive. However, where departments find - perhaps because of a change in their duties - that they will regularly require authorisation, they should request the Chief Executive to appoint an Authorising Officer specifically for their department.

3.2 Recording and Registration of Authorisations, etc

All departments carrying out surveillance activities must maintain a record of applications made for directed surveillance, together with a record of the consent, refusal, renewal, cancellation, review or changes in circumstances in the style of the forms approved by the Home Office/OSC and adopted by Angus Council for this purpose (see Appendix Two). These forms are available on the council's RIP(S)A intranet page. Notes for Guidance to assist completion of these forms have also been prepared and, likewise, are available on the council's RIP(S)A intranet page. These notes only represent practical guidance on completion of these forms, however, and are subordinate to these policy guidelines. These forms must be retained safely and securely.

Each public authority must hold a centrally retrievable record of all authorisations. In Angus, this is held by Legal and Democratic. The “Register of Authorisations” must be completed for each investigation. Each authorisation must obtain a Unique Reference Number from Legal and Democratic before an authorisation is finally approved. Once the investigation has been authorised, a copy of the completed authorisation form should be forwarded to Legal and Democratic immediately. Copies of any amending documentation should also be forwarded to Legal and Democratic. All copy forms must be sent to the Service Leader - Legal in sealed envelopes marked "Private and Confidential" and addressed to the Service Leader - Legal. Where applicants are working remotely and not able to produce a hard copy Application form, they should apply a wet signature to the application and convert it to a PDF document before sending it to an Authorising Officer for authorisation.

The register and forms will be monitored for cross-department consistency by the Service Leader - Legal and will have to be produced in the event of an inspection by the IPCO. These forms represent evidence of the council's compliance with RIP(S)A and the Codes of Practice and, as such, care should be taken in the completion and logging of them. Departments must ensure that the forms are easily retrievable and held in a central location in each department as it is likely that only two weeks' notice will be given before the IPCO carry out an investigation. Information from the IPCO suggests that inspections will take place annually.

An annual return of all authorisations must be made by the Service Leader - Legal as at 31 March of each year. A fully completed list will be requested in early April of each year.

3.3 Grant or Refusal of Authorisations

IPCO may require an Authorising Officer to justify his/her decision to grant a request, so authorisation should never be granted automatically. Evidence of reasoned refusal of requests is also vital in displaying compliance with the law. Consideration must be given to the principles of surveillance contained in Part B of Appendix One.

The Authorising Officer's job is to be satisfied that the officer seeking approval has correctly applied the tests set out in Section 2 of this guidance, so that the surveillance:-

- is for lawful purpose and does not stray beyond the permissible bounds of directed surveillance;
- is necessary (i.e. there are no other reasonable alternatives);
- is proportionate (i.e. intrusion has been minimised compared to the end sought); and
- has been properly planned to minimise the risk of collateral intrusion or collection of confidential information.

Only if actively satisfied about all of these points should the authorisation be granted.

The other **critical** part of the Authorising Officer's job is to specify exactly what the terms of the authorisation granted are. Section 6(4)(a) of RIP(S)A requires the Authorising Officer to describe and specify what they are granting. This may or may not be the same as requested by the applicant. For the benefit of those operating under the terms of an authorisation, or any person who may subsequently review or inspect an authorisation, it is essential to produce, with clarity, a description of that which is being authorised (i.e. who, what, where, when and how). The Authorising Officer should as a matter of routine state explicitly and in his own words what is being authorised, and against which subjects, property or location. Mere reference to the terms of the application is inadequate.

Case Law (see *Gilchrist -v- HMA 2004 SLT 1167; 1 JC 34)* has clarified that the want of a proper explanation as to the terms of the authority (either within the Authorising Officer's statement or incorporated there by direct reference to elsewhere in the application) may invalidate the authorisation. The notes for completion are also available on the Council's RIP(S)A intranet page web pages which give further practical guidance on content of the Authorising Officer's statement.

Case Law (see R –v- Sutherland [2002] EW Misc 1 (EWCC)) has re-enforced the requirement that all officers who are to conduct any form of activity under the terms of an authorisation **must** be able to demonstrate (to an auditable standard) that they have seen and understood the authorisation which has been granted. Departments must ensure that all officers who are to conduct any form of activity under the terms of an authorisation receive copies of the authorisation granted and record their receipt of this and their understanding of the terms of that authorisation.

3.4 Duration, Renewal and Cancellation of Authorisations

By law, an authorisation for directed surveillance lasts for three months. If the justification for carrying out the surveillance ceases to apply, the authorisation should be cancelled and a record kept of the cancellation and the reasons for the cancellation. For the avoidance of doubt all amended forms, including renewals and cancellations must be forwarded to the Service Leader - Legal.

An authorisation for the use of a CHIS will last for a maximum of 12 months.

If the surveillance is to be continued for longer than the original period, a renewal must be authorised. Renewal applications must highlight the fact that what is sought is a renewal and should have attached the original authorisation and any previous reviews and/or renewals. The tests applicable to renewals are identical to those for initial applications.

In the case of authorisations for directed surveillance, there should be a review by the Authorising Officer within a month. This review should note whether any significant evidence has been acquired by the surveillance and whether, against that background, continued surveillance can still be justified. Review dates should be noted on the authorisation form.

3.5 Security and Retention of Documents

Documents created under this procedure are highly confidential and must be treated as such. Departments must make proper arrangements for their retention, security and destruction, in accordance with the requirements of the Code of Practice, the General Data Protection Regulations and the Data Protection Act 2018, the Procedure for Authorisation of Covert Surveillance and Chapter 8 of the Scottish Government's Code of Practice on Covert Surveillance and Property Interference. Refusals, as well as approved applications, must be retained. The Code of Practice recommends retaining the authorisations for at least three years (longer if required for ongoing proceedings).

In accordance with Guidance, documents will be inspected periodically by the Service Leader - Legal to ensure that a consistent approach is being adopted by different council departments. IPCO also has statutory powers of inspection and all records (applications, authorisations and refusals) must be available for inspection. No record should be destroyed until after an IPCO Inspector has had the opportunity to see them.

Each department carrying out surveillance activities must make appropriate arrangements for the secure storage of authorisations and refusals.

The Service Leader - Legal shall maintain a register of current and past authorisations. Applicant officers shall ensure that sufficient information is provided to keep this up to date.

In addition to the above, IPCO has identified that many organisations are retaining data for longer than is necessary or appropriate for a number of reasons. Firstly, in many cases authorities have not fully implemented data retention and disposal policies, secondly, many authorities operate with a culture of comprehensive retention to prevent operational data loss, and finally, systems used to transfer and securely store data may not promote or enable appropriate disposal processes.

An example of this has been provided:-

"consider that an authority seeks and is granted a directed surveillance authorisation. Under that authorisation, surveillance is conducted for a period of time and provides information to meet the objectives of the investigation. As part of the investigation, one officer emails the results of the surveillance to a colleague and their manager, both of whom save a copy on their desktop and in Outlook for future reference. The officer also emails the product to a legal colleague so that the product may be used as evidence during criminal proceedings, it is therefore disclosed to a court and retained in a password protected file for further use in the event of an appeal. At this point, no decision is taken as to how long that data should be retained, and the copies on both Outlook and the desktops are retained.

Although this example demonstrates legitimate use of the data for investigative and evidential use of the data, this approach is unlikely to be compliant with the code of practice for surveillance. The data pathway described includes retention on a personal desktop and in Outlook as well as a password-protected evidential

copy. In this example, no retention, review or disposal process is in place for either pathway. In cases such as this, my inspectorate have found that data is being retained longer than is necessary, and at times indefinitely. I urge you to review your obligations under IPA and RIPSA and to revisit the safeguards in the Codes of Practice to ensure that appropriate policies and processes are in place within your authority."

Dissemination, copying and retention of material must be limited to the minimum necessary for authorised purposes. In accordance with the Code of Practice, something is necessary if the material;

(i) is, or is likely to become, necessary for any of the statutory purposes set out in RIP(S)A Act in relation to covert surveillance;

(ii) is necessary for facilitating the carrying out of functions of public authorities under those Acts;

(iii) is necessary for facilitating the carrying out of any functions of the IPC of the Investigatory Powers Tribunal;

(iv) is necessary for the purposes of legal proceedings; or

(v) is necessary for the performance of any functions of any person or under any enactment.

Material obtained as a result of a surveillance operation may be used as evidence in criminal proceedings. It is important that the continuity and integrity of evidence is preserved during and after an operation. The Council should be able to demonstrate how the evidence has been obtained and preserved. This means that as part of the cancellation meeting Applicants should include in the Cancellation Form; what information was obtained as a result of the operation, how they will safeguard it until it is destroyed, deleted or shared with a relevant enforcement agency e.g. Procurator Fiscal, as part of criminal proceedings and who it will be shared with (where this is possible).

Information obtained through a covert surveillance and all copies, extracts, summaries related to that operation should be destroyed in accordance with the Applicant's Service/ Cluster's retention policy in relation to the particular function they are carrying out.

4. Central Record of all Authorisations

A centrally retrievable record of all authorisations should be held by the Service Leader - Legal and regularly updated whenever an authorisation is granted, renewed or cancelled. The record should be made available to the relevant Inspector from the Investigatory Powers Commission, upon request. These records should be retained for a period of five years from the ending of the authorisation and should contain the following information:

- The type of authorisation.
- The date the authorisation was given.
- Name and rank/grade of the Authorising Officer.
- The unique reference number (URN) of the investigation or operation.

- The title of the investigation or operation, including a brief description and names of subjects, if known.
- Whether the urgency provisions were used, and if so why.
- If the authorisation is renewed, when it was renewed and who authorised the renewal, including the name and rank/grade of the Authorising Officer.
- Whether the investigation or operations is likely to result in obtaining confidential information as defined in this Code of Practice
- The date the authorisation was cancelled.

In all cases, services should maintain for a period of three years the following documentation which need not form part of the centrally retrievable record:

- A copy of the application and a copy of the authorisation together with any supplementary documentation and notification of the approval given by the Authorising Officer.
- A record of the period over which the surveillance has taken place.
- 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.

5. OVERSIGHT OF COVERT SURVEILLANCE ARRANGEMENTS

IPCO provides independent oversight of the use of powers contains within RIP(S)A.

IPCO conduct Inspections of each public authority on a triannual basis during which (normally) a sample of applications for authorisation are normally reviewed by the Inspector in detail.

Elected members on the Audit Risk and Scrutiny Committee will receive reports on a quarterly basis regarding RIP(S)A activity and compliance. A review of the RIP(S)A protocol and procedure will also considered annually by the Policy and Resources Committee.

Additional oversight of authorisations is also provided by the Information Governance team, who audit all authorisations made and provide feedback to both Applicants and Authorising Officers on the quality and clarity of an application. This audit occurs after the application form has been authorised, as it is the Authorising Officers responsibility to be satisfied as to the quality, necessity and legality of the application.

APPENDIX ONE - INTERPRETATION

PART A - GLOSSARY OF TERMS

(a) Covert surveillance

Surveillance is covert if, and only if, it is carried out in a manner calculated to ensure that the subject of the surveillance is unaware that it is taking place (see Section 1(8)(a) of RIP(S)A).

(b) Directed surveillance

Surveillance is directed if it is covert but not intrusive and is undertaken for the purpose of a specific investigation in such a manner as is likely to result in obtaining private information about a person and is otherwise than by way of an immediate response to events, the nature of which is such that it would not be reasonably practicable for an authorisation to be sought (see Section 1(2) of RIP(S)A).

(c) Covert human intelligence source

A "CHIS" is a person who establishes or maintains a relationship with another in order to obtain information covertly (see Section 1(7) of RIP(S)A).

(d) Intrusive surveillance

Intrusive surveillance is covert surveillance carried out in relation to anything taking place on any residential premises or in any private vehicle, which involves the presence of an individual on the premises or in the vehicle or is carried out by means of a surveillance device which consistently provides information of the same quality and detail as could be obtained from a device naturally present in the residential premises or vehicle (see Section 1(3) and (5) of RIP(S)A).

(e) Private information

This includes any information relating to a person's private or family life (see Section 1(9) of RIP(S)A). Case Law has clarified that:-

- “private life” is not susceptible to a clear definition;
- the term does, however, justify a wide interpretation; and
- the term will include professional or business interests.

PART B - PRINCIPLES OF SURVEILLANCE

(a) Lawful Purposes

Covert surveillance can only be carried out where it is necessary to achieve one or more of the permitted purposes (as defined in RIP(S)A). Covert surveillance must therefore be:

- for the purpose of preventing or detecting crime or the prevention of disorder; or

- in the interests of public safety; or

- for the purpose of protecting public health.

Employees carrying out surveillance must not cause damage to any property or harass any person.

(b) Necessity

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

(c) Effectiveness

Planned covert surveillance shall be undertaken only by, or under the supervision of, suitably trained or experienced employees.

(d) Proportionality

The use and extent of covert surveillance shall not be excessive, i.e., all covert surveillance must be in proportion to the significance of the matter being investigated. If there is a way of obtaining the information in a less intrusive manner, then that less intrusive manner should be used.

(e) Intrusive Surveillance

No activities shall be undertaken that come within the definition of "intrusive surveillance", i.e. if the activity involves surveillance of anything taking place in residential premises or in a private vehicle. (However, see 2.4 above.)

(f) Collateral Intrusion

Reasonable steps shall be taken to minimise the acquisition of any information which is not directly necessary for or relevant to the purposes of the investigation being carried out.

(g) Authorisation

All directed surveillance must be authorised in accordance with the procedures described above.

APPENDIX TWO – RIP(S)A FORMS

Notes for Completion of Forms

Directed Surveillance

DS 1 Application for Authorisation DS 2 Application for Renewal

DS 3 Cancellation
DS 4 Review
DS 5 Change of Circumstances

Covert Human Intelligence Source

CHIS 1 Application for Authorisation CHIS 2 Application for Renewal
CHIS 3 Cancellation
CHIS 4 Review
CHIS 5 Change of Circumstances

APPENDIX THREE - CHIS SOURCE RECORDS

PART A - EXTRACT FROM SSI 2002/205

Particulars to be contained in records

"**3.** The following matters are specified for the purposes of section 7(6)(d) of the 2000 Act (as being matters particulars of which must be included in the records relating to each source):-

(a) the identify of the source;

(b) the identity, where known, used by the source;

(c) any relevant investigating authority other than the authority maintaining the records;

(d) the means by which the source is referred to within each relevant investigating authority;

(e) any other significant information connected with the security and welfare of the source;

(f) any confirmation made by a person granting or renewing an authorisation for the conduct or use of a source that the information in paragraph (e) has been considered and that any identified risks to the security and welfare of the source have where appropriate been properly explained to and understood by the source;

(g) the date when, and the circumstances in which, the source was recruited;

(h) the identities of the persons who, in relation to the source, are discharging or have discharged the functions mentioned in section 7(6)(a) to (c) of the 2000 Act or in any order made by the Scottish Ministers under section 7(2)(c);

(i) the periods during which those persons have discharged those responsibilities;

(j) the tasks given to the source and the demands made of him or her in relation to their activities as a source;

(k) all contacts or communications between the source and a person acting on behalf of any relevant investigating authority;

(l) the information obtained by each relevant investigating authority by the conduct or use of the source;

(m) any dissemination by that authority of information obtained in that way; and

(n) in the case of a source who is not an undercover operative, every payment, benefit or reward and every offer of a payment, benefit or reward that is made or provided by or on behalf of any relevant investigating authority in respect

of the source's activities for the benefit of that or any other relevant investigating authority."

PART B - EXTRACT FROM CHIS CODE OF PRACTICE

"7.6. In addition, records or copies of the following, as appropriate, should be kept by the relevant authority for at least three years:

- a copy of the authorisation together with any supplementary documentation and notification of the approval given by the Authorising Officer;
- a copy of any renewal of an authorisation, together with the supporting documentation submitted when the renewal was requested;
- the reason why the person renewing an authorisation considered it necessary to do so;
- any authorisation which was granted or renewed orally (in an urgent case) and the reason why the case was considered urgent;
- any risk assessment made in relation to the CHIS;
- the circumstances in which tasks were given to the CHIS;
- the value of the CHIS to the investigating authority;
- a record of the results of any reviews of the authorisation;
- the reasons, if any, for not renewing an authorisation;
- the reasons for cancelling an authorisation;
- the date and time when any instruction was given by the Authorising Officer that the conduct or use of a CHIS must cease; and
- a copy of the decision by a Judicial Commissioner on the renewal of an authorisation beyond 12 months"