WEST DUNBARTONSHIRE COUNCIL

5th EDITION

POLICY GUIDELINES

ON

COVERT SURVEILLANCE,
COVERT HUMAN INTELLIGENCE SOURCES

AND

SOCIAL MEDIA USE

REVISED MAY 2024

[TABLE OF CONTENTS BEING PREPARED]

1.

PART A: COVERT SURVEILLANCE

1. INTRODUCTION AND BACKGROUND

1.1 The Human Rights Act 1998, which came into force in October 2002, gave domestic effect to the European Convention on Human Rights (ECHR). Section 6 of the 1998 Act provides that it is unlawful for public authorities to act in any way which is incompatible with a Convention right.

There are situations in which local authority employees, in the course of their duties, will have to carry out investigations and activities which, by the nature of the investigation, are covert. It is essential that covert investigations are therefore compatible with Article 8 of ECHR which states that *everyone has the right to respect for family and private life, his home and correspondence.*

In Convention terms, the idea of private life is broad.

It is therefore clear that most covert surveillance operations interfere with this right of privacy. However, the rights guaranteed in Article 8 are not unfettered - interference with the right to privacy can be justified if:-

(i) in accordance with the law;

(ii) it is necessary to pursue a legitimate aim (public interest); and

(iii) the interference is proportionate to the legitimate aim - the interference with the right of privacy is not greater than is necessary to achieve the aim.

The Regulation of Investigatory Powers (Scotland) Act 2000 (RIP(S)A) provides, for the first time, a legal framework for covert surveillance by public authorities and an independent inspection regime to monitor these activities. The primary purpose of RIP(S)A is therefore to ensure compliance with Article 8 in relation to covert surveillance. Therefore, if local authority investigators, in the course of their duties, ensure that they obtain authorisation **and** that they act in accordance with that authorisation any interference with the right of privacy will be in accordance with the law and the activities and evidence of investigating Officers will be lawful for all purposes.

The purpose of this policy is, therefore, to advise and ensure that employees and Authorising Officers are aware of the terms of RIP(S)A and that any covert surveillance, whether direct surveillance or use of a covert human intelligence source, is necessary and proportionate in terms of application for and the granting of authorisations in terms of the Act. This Policy Document should be read in conjunction with the following Codes of Practice;

1. Code of Practice on Covert Human Intelligence Sources: http://www.scotland.gov.uk/Topics/Justice/public-safety/Police/policepowers/17206/7789

2. Code of Practice on Covert Surveillance: http://www.scotland.gov.uk/Topics/Justice/public-safety/Police/policepowers/17206/7789

3. Any guidance issued by Office of the Surveillance Commissioner issued from time to time. https://www.gov.scot/publications/covert-surveillance-property-interference-code-practice/

1.2 Scope of Policy

Firstly, RIP(S)A only applies to covert surveillance. Basically, surveillance is covert where it is carried out in such a way that anyone subject to that surveillance is unaware that the surveillance is taking place. The Act does not apply to any surveillance which is overt. For example, surveillance will generally be overt where CCTV cameras are used since members of the public should have been made aware of such use by placed notices. Surveillance is also overt where the person subject to the surveillance has been made aware that surveillance is being carried out. However, where a public authority uses a CCTV system for a specific investigation, authorisation for Directed Surveillance may be necessary. If any investigating Officer is in doubt, legal advice should be sought.

Moreover, if an operator of any Council CCTV system is approached by any other employee or other agency requesting that the operator undertake Directed Surveillance using CCTV, the operator is required to obtain a written copy of the RIP(S)A authorisation prior to such use. This authorisation must detail the use of a specific camera system for the purpose of Directed Surveillance. The authorisation must be signed by one of the Council's Authorising Officers or, in the case of Police, an officer of at least the rank of Superintendent. In urgent cases, an authorisation approval by a Police Officer of at least the rank of Inspector can be accepted. A copy should be kept and the original forwarded to Manager of Legal Services for noting in the Central Register.

Secondly, the Act does not make unauthorised activities unlawful nor does it compel the obtaining of an authorisation or provide sanctions for failing to do so. However, this having been said, the consequences of failing to obtain an authorisation can be that the actions of individual Officers are rendered unlawful in terms of the Human Rights Act. As a result, a court may question the admissibility of evidence obtained in such a way. It is, therefore, essential that Investigating Officers obtain authorisation and comply with the terms of that authorisation.

There are three types of surveillance, as defined within RIP(S)A, which can be summarised as follows:-

1.2.1 Intrusive Surveillance

This is covert surveillance that is 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.

There is no provision within RIP(S)A whereby local authorities may be authorised to carry out any form of intrusive surveillance. As a matter of policy, local authority officers **must not** engage in intrusive surveillance. As a result of this it is important that all employees are completely clear as to the definition of intrusive surveillance. Examples sometimes help for clarification;

What if surveillance of a residential premises or surveillance of a private vehicle takes place using a device placed outwith the actual premises or outwith the vehicle. Is this intrusive surveillance?

This would not be intrusive surveillance unless the information obtained is consistently of the same quality as the device would have provided had it been actually present in the home or vehicle. Thus, activities such as filming goods being sold from the back of a car is unlikely to be intrusive surveillance. The monitoring of the level of noise generated by an anti-social tenant would not be intrusive so long as the information is not consistently of the same quality as a device actually present in that home would have provided. Officers need to consider more than just the technical capability of the recording device. Other factors, such as thin party walls and poor sound insulation between properties, may lead to the recorded quality being as good as if the device was actually present in the target house.

This does not mean that authorisation should not be obtained, what it does mean is that it is not intrusive surveillance. It may still be Directed Surveillance.

Devices such as listening and audio visual equipment carried into the residential premises or a private vehicle by a covert human intelligence source do not constitute intrusive surveillance so long as that covert human intelligence source has been invited in to the premises/vehicle. However, the device must not be left behind when the covert human intelligence source leaves the premises or vehicle.

It is the two remaining categories of covert surveillance which principally concern local authorities, namely Directed Surveillance and the conduct and use of a Covert Human Intelligence Source (CHIS).

1.2.2 Directed Surveillance

Directed Surveillance is defined as surveillance which is covert but not intrusive and is undertaken:-

(a) for the purpose of a specific investigation or specific operation; and

(b) in such a manner as is likely to result in the obtaining of private information about a person. That person does not specifically need to be the person subject to the investigation. It is simply private information about a person. RIP(S)A states that 'private information' about a person "includes information relating to the person's private or family life". However, the use of the word 'includes' suggests that the definition should be interpreted quite widely. It could, for example, include information about a person's professional or business activities which is not publicly known.

It is important to note that any overt observations do not require authorisations under RIP(S)A.

A general observation forming part of a Trading Standards Officer's duties do not require authorisation. For example, a Trading Standards Officer might covertly observe and then visit a shop as part of their enforcement function to verify the supply or level of goods or services that may be liable to a restriction. Such an observation could involve the use of equipment, such as binoculars or the use of cameras where this does not involve a systematic surveillance of an individual. Each case, of course, must be taken on its own merits. When an authorising officer is in doubt as to whether or not this may be Directed Surveillance, legal advice should be sought.

Directed Surveillance is for the purposes of a specific investigation or a specific operation. For example, unplanned observations in immediate response to unfolding events are unlikely to require an authorisation.

Authorisations must be in writing. However, there is an exception whereby authorisations may be issued orally in urgent cases provided the Authorising Officer's entitlement to grant authorisations is not limited to urgent cases. 'Urgent' is defined in the Code of Practice. A written record of any oral authorisation should be made as soon as reasonably practicable.

1.2.3 Covert Human Intelligence Source (CHIS)

A CHIS establishes or maintains, in effect cultivates a personal relationship with others to obtain information, provide access to information for someone else or discloses information obtained through that relationship. The other party has to be unaware of the purpose of the relationship. The authorisation procedures are similar to those in Directed Surveillance, however, additional rules apply to the use of a CHIS. Council Officers making undisclosed site visits or test purchases are not CHISs and as such do not require any authorisation. Having said that, a member of the public could become a CHIS if they covertly obtain information after consulting and obtaining instructions from Council Officers. Members of the public who volunteer information as part of their civic duty are not CHISs.

The Codes of Practice issued by the Scottish Executive should be read in conjunction with Directed Surveillance and CHISs. See Part B of this Policy for further detail.

1.2.4 Scope of the Procedure

This procedure applies in all cases where "Directed Surveillance" is being planned or carried out. As indicated above, Directed Surveillance is defined by RIP(S)A as covert surveillance undertaken "for the purpose of a specific investigation or a specific operation" and "in such a manner as is likely to result in the obtaining of private information about a person" whether or not that person is the target of the operation and other than by way of an immediate response to events or circumstances (Section 1(2) RIP(S)A).

1.3 Principles of Surveillance

In planning and carrying out covert surveillance, Council employees have to comply with the following principles. Furthermore, Authorising Officers have to be particularly stringent in detailing the boundaries of the surveillance activity which they as Authorising Officers are sanctioning.

Investigating Officers and Authorising Officers should, therefore, ask themselves the following questions when asking/granting authorisation for Directed Surveillance and a CHIS.

1.3.1 Is there a lawful purpose?

Covert surveillance shall only be carried out where **necessary** to achieve one or more of the permitted purposes as defined within RIP(S)A. In relation to Local Authorities, it is for the following reasons:-

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

(b) In the interests of public safety;

(c) For the purpose of protecting public health; and

(d) For any other purpose prescribed in an order made by the Scottish Ministers.

1.3.2 Is the surveillance necessary?

Covert surveillance can only be undertaken where there is no reasonable and effective alternative way of achieving the desired objectives. The question of necessity also has to be viewed in all the circumstances of the specific case before the Authorising Officer.

1.3.3 Is the surveillance proportionate?

The use and extent of covert surveillance should not be excessive. This means that the surveillance should be proportionate to the significance of what is being investigated. Basically, if the same lawful purpose could be reached by less infringement of a citizen's rights then that lesser path should be taken. When assessing proportionality, employees and Authorising Officers must also consider the seriousness of the alleged behaviour/breach. Minor misdemeanours may not be sufficient to warrant a large surveillance operation. On occasions, sentencing powers in criminal offences may be a useful guide. However, having said that some regulatory offences can have life

threatening consequences, for example, the sale of contaminated foods or dangerous goods and this could result in the surveillance being proportionate. The factors which should be addressed in the decision making process regarding proportionality are whether or not there were relevant and sufficient reasons advanced in support of the application. Was there a less intrusive means of detection/investigation? Was there procedural fairness in the decision making process and were safeguards against abuse made clear?

When addressing the concept of *proportionality* all Applicants and Authorising Officers should have in mind three basic concepts for consideration.

1. That the use of covert surveillance is a proportionate response to the level of mischief being investigated.

2. That the degree of intrusion upon the target and collaterally is not excessive.

3. That all other reasonable options for gathering the evidence have been considered and rejected.

All Authorising Officers should make their thinking and decision making clear when authorising surveillance. Each of these concepts have to be addressed within the form and justified.

1.3.4 Will the proposed surveillance be intrusive?

If the surveillance comes within the definition "intrusive" surveillance in terms of RIP(S)A then no activity can be authorised by any Authorising Officer. As a matter of policy, local authority officers **must not** engage in intrusive surveillance.

1.3.5 Could there be collateral intrusion**?**

Reasonable steps should be taken to minimise the possibility that information is obtained on other persons who are not directly involved in the operations. This is also a factor to consider when making the proportionality test. Again, this is an issue which Authorising Officers need to address specifically in each authorisation.

1.3.6 Could confidential material be obtained?

Confidential material includes matters subject to legal privilege, for example, this can be information passed between a client and their legal advisor and surveillance should be planned in such a way as to avoid confidential material being obtained. Confidential material should be destroyed once it is no longer necessary for the specific purpose of the surveillance. In particular. the proportionality test has to be applied at all times. Applications where a significant risk of acquiring confidential material has been identified shall always require the approval of the Chief Executive or, in their absence, Chief Officer.

2. THE AUTHORISATION PROCESS

2.1 General Rules on Authorisations

An authorisation under RIP(S)A will provide lawful authority for a public authority to carry out covert surveillance. Responsibility for authorisations is described in the Regulation of Investigatory Powers (Prescription of Officers, Ranks & Positions) (Scotland) Order 2000. Authorisations must be granted by an 'Assistant Head of Service or Investigation Manager' or above. In effect, this means a grant or refusal by the Chief Executive, an officer of the rank of Chief Officer or Head of Service or Section Head. Authorisation to access "confidential material" should normally be signed by the Chief Executive.

Authorising Officers are noted at Appendix 1.

Before authorising surveillance, any Authorising Officer must be satisfied that the activities for which authorisation is sought are necessary and proportionate to what is hoped to be achieved.

Authorisation is necessary if it satisfies the following grounds:-

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

(b) In the interests of public safety;

(c) For the purpose of protecting public health; and

(d) For any other purpose prescribed in an order made by the Scottish Ministers.

Once the Authorising Officer has considered that the activity is necessary, he/she must then address the question of proportionality.

The whole question of proportionality is to seek a balance between what is being sought and the means used to achieve this. If there is an easier or less intrusive means of obtaining the information then the authorisation cannot be proportionate to what is being sought and therefore should be refused. The matters referred to in paragraph 2.1 should be taken into account by the Authorising Officers. Moreover, the Authorising Officer should be aware that what he/she is authorising is the surveillance operation itself and not the actual event which has given rise to the operation. The Authorising Officer should detail any parameters/boundaries of the surveillance activity which they are sanctioning. Authorisations must be given in writing. In urgent cases only, an Authorising Officer may approve oral applications. An application, in writing, indicating the reasons why an oral authorisation was sought must then be made as soon as reasonably practicable. In any case, an oral authorisation will expire after 72 hours. If surveillance is to continue after the 72 hours a further application, in writing, must be made and is for a period of three months. An urgent oral application is only available where delay would endanger life or jeopardise the investigation.

In accordance with the Code of Practice, authorisations will last three months. The person responsible for authorising a surveillance must ensure that the authorisation is reviewed at least monthly and those authorisations are no longer needed or appropriately cancelled. Authorisations must be cancelled, they should not be allowed to lapse.

Applications for authorisation are made in writing using the appropriate form. The Authorising Officer should then note the time and date of his or her grant or refusal of the application on the form.

Confidential Material

Applications where a significant risk of acquiring confidential material has been identified shall always require the approval of the Chief Executive or, in their absence, a Chief Officer.

As indicated earlier, confidential material consists of:-

- matters subject to legal privilege, for example, between professional legal adviser and client;

- confidential personal information, for example, relating to a person's physical or mental health; or

- confidential journalistic material.

Such applications shall only be granted in exceptional and compelling circumstances where the Authorising Officer is fully satisfied that the surveillance is both necessary and proportionate in these circumstances. In accordance with the Code of Practice such authorisations will last one month. Where any confidential material is obtained, then the matter must be reported to the Office of Surveillance Commissioners during the next inspection and any material obtained made available to them if requested.

2.2 Test Purchases - Juvenile

Where a juvenile is used there should be full consultation with the child/young person and the child/young person's parent/guardian on all of the issues involved. Certain factors should be taken into account:-

(a) Participation must be entirely voluntary and have the consent of the child/young person and his/her parents or guardians.

(b) The child/young person's parent/guardian must fully understand the nature of the task involved and give written consent. It is prudent to mention that should the young volunteer have to give evidence in Court then this would be conducted in such a manner as to minimise any risks. The protection offered to child witnesses under the law when giving evidence for example, Vulnerable Witnesses (Scotland) Act 2004, should be discussed with the parents where appropriate.

The anonymity of the child/young person is an important consideration during any test purchase. With regard to test purchases a child/young person should not be asked to make test purchases in an area where they are likely to be recognised, such as near their home, school, club etc.

The child/young person should be supervised at all times. A minimum of two Officers should accompany the child during the exercise. One Officer, ideally of the same sex as the child/young person, should be responsible for the child/young person's safety and welfare for the duration of the exercise.

Reference should be made to the Scottish Test Purchasing Protocol for age restricted products. West Dunbartonshire Council keeps under review the practice of juvenile test purchase operations and whether an authorisation is applicable, taking into account the specific proposed surveillance and how this is to be achieved in each case.

2.3 Combined Authorisations

A single authorisation may combine two or more authorisations under RIP(S)A. For example, a single authorisation may combine authorisations for Directed Surveillance and a CHIS. In such cases the provisions applicable to each of the authorisations have to be considered separately.

2.4 Duration of Authorisation

(a) Directed Surveillance

A written authorisation granted by an Authorising Officer will cease to have effect (unless renewed) at the end of a period of three months beginning with the day on which it took effect.

Urgent oral authorisation or written authorisations granted by a person who is only entitled to act in urgent cases will, unless renewed, cease to have effect after 72 hours beginning with the time when the authorisation was granted.

(b) Covert Human Intelligence Sources

In the case of a CHIS, a written authorisation will, unless renewed, cease to have effect at the end of a period of 12 months beginning with the day on which it took effect. Urgent oral authorisations are again the same as Directed Surveillance, that is 72 hours.

The authorisation should be forwarded to the Manager of Legal Services for filing on the Central Register.

Cancellation, **which is discussed in the next paragraph**, should be used as a principal and best desirable means of the termination of an authorisation. Also best practice would indicate that originals of all applications, authorisations, reviews, renewals and cancellations should be lodged with the central record.

2.5 Documents

This procedure uses the following documents **which shall be used by all departments:-**

1. Application for authority for Directed Surveillance

The Applicant in all cases should complete this, including where oral authorisation was first sought. It is effective from the time that approval is given.

2. Application for renewal of Directed Surveillance authority

This form should be completed where a renewal for authorisation is applied for.

3. Application for a review of Directed Surveillance authority

The Authorising Officer shall complete this when carrying out reviews of authorisation.

4. Cancellation of a Directed Surveillance

The Applicant and Authorising Officer should complete this when the authorisation ceases to be either necessary or appropriate.

2.6 Cancellation of Directed Surveillance

The Applicant and the Authorising Officer should complete this when the authorisation ceases to be either necessary or appropriate.

2.7 Review of Directed Surveillance

The Authorising Officer should complete this when carrying out reviews of the authorisation.

2.8 Renewal and Cancellation of Authorisations

If, however, the reasons justifying carrying out the surveillance cease to apply, then the authorisation should be cancelled and the cancellation form forwarded to the Manager of Legal Services for filing on the Central Register.

If surveillance is to be continued for longer than the original period authorised, it is necessary to have a renewal authorised. The tests applicable to renewals are identical to those for initial applications. Applications for the renewal of the conduct or use of a CHIS should not be granted unless the Authorising Officer is satisfied that a review has been carried out. The results of the review 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 the review should be recorded on the authorisation record.

Reviews

Regular reviews of authorisations should be undertaken to assess the need for surveillance to continue. The results of a review should be recorded on the Central Record of Authorisations. The Authorising Officer should determine how often a review should take place. This should be as frequently as considered necessary and practicable.

Cancellation

The Authorising Officer who granted or last renewed the authorisation must cancel it if that officer is satisfied that the surveillance no longer meets the criteria upon which it was authorised. When the Authorising Officer is no longer available, this duty will fall on the person who has taken over the role of Authorising Officer. An authorisation could not be allowed to simply lapse, it should be cancelled.

2.9 Central Record of all Authorisations

The Manager of Legal Services shall maintain a register of current and past authorisations and of any applications for authorisations that have been refused. Each department will provide the Council Solicitor with all original documentation relating to authorisations under the Regulation of Investigatory Powers (Scotland) Act 2000, including cancellations, renewals and reviews within three working days of the action being taken. Authorising Officers shall ensure that sufficient information is provided to keep this up to date.

Each authorisation will be given a unique reference number prefaced by the departmental number in brackets. The Central Register will contain the following information:-

- Type of authorisation eg Directed Surveillance or Covert Human Intelligence Source.
- Start date of the authorised activity.
- Whether the application was authorised or refused.
- Date of authorisation/refusal.
- Name and title of the Authorising Officer.
- Title of the investigation or operation, if known, including a brief description and names of subjects.
- Whether the urgency provisions were used and if so why.

- Confirmation that the authorising officer did not authorise their own activities.

- Date of review.

- Date of renewal and who authorised the renewal.

- Date of cancellation.

- Whether the investigation is likely to result in obtaining confidential information as defined in the Code of Practice.

- Whether in the case of a CHIS the source is a juvenile or “vulnerable" person as defined in the Code of Practice.

The Manager of Legal Services will provide regular monitoring information to departments and produce an annual report in relation to the Central Register.

The Central Register must be retained for a period of at least three years from the ending of the authorisation, or for a further suitable period if relevant to pending court proceedings.

A centrally held record of all authorisations is held by the **Manager of Legal Services, Municipal Buildings, College Street, Dumbarton G82 1NR.** This record is regularly updated whenever an authorisation is granted, renewed or cancelled. The record is retained in a locked cabinet and this record can be made available to the relevant Commissioner or an Inspector from the Office of the Surveillance Commissioners upon request. All records should be retained for a period of at least three years from the ending of the authorisation. Furthermore, proper records must be kept of the authorisation and use of a source, detailing all the arrangements in place for ensuring that there is, at all times, a person with responsibility for maintaining a record of the use made of the source until such times as cancellation.

It is recommended that the applicant obtain from Legal Services, before completing an authorisation, next sequential unique reference number prior to completing any authorisation form. This will ensure that in the event of an authorisation being refused, the central record will contain a note of that refusal. This will assist with more effective oversight of processes.

2.10 Training

Each department is responsible for ensuring that their staff receive adequate training to deal with the authorisation process and any enquiries. Advice is, however, available as required from Legal Services.

2.11 Public Access

Copies of the underlying Policy and Codes of Practice are available for public reference at Legal Services at West Dunbartonshire Council, Municipal Buildings, College Street, Dumbarton G82 1NR, email: Legal.LitigationandSupport@west-dunbarton.gov.uk. Please note that access is by appointment.

2.12 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, benefits agency, Customs and Excise, etc. It is for the organisation seeking the assistance from West Dunbartonshire Council to ensure that they have the appropriate authorisations in place. Best practice suggests that such authorisations should be shown to Council staff involved. If these are not written, confirmation should be given that authorisations have been duly granted. If, however, this is part of a joint operation and the Council is carrying out its own surveillance, Council Officers should arrange for their own authorisations to be put in place.

2.13 Complaints

Any member of the public who is unhappy or dissatisfied with the conduct of any covert surveillance has a right to complain to the Investigatory Powers Tribunal. The individual can also complain through the Council's own Complaints Procedure.

Details of the Complaints Procedure are available for public reference at Legal Services.

The Regulation of Investigatory Powers Act 2000 (the “UK Act”) establishes an independent tribunal. This tribunal has full powers to investigate any complaints and decide any cases within the United Kingdom, including complaints about activities carried out under the provisions of the Regulation of Investigatory Powers (Scotland) Act 2000. Details of the relevant Complaints Procedure can be obtained from the Investigatory Powers Tribunal, PO Box 33220, London, SW1H 9ZQ.

2.14 Conclusion

In conclusion, RIP(S)A regulates surveillance activity with the aim that the activity will be compliant with the European Convention of Human Rights (ECHR) and that there will be no difficulty in admitting any such evidence as part of a criminal trial.

If the terms of RIP(S)A have been complied with and the dual principles of necessity and proportionality have been addressed, then any interference with any individual’s rights to privacy will be in accordance

with the law. The activities and thereafter evidence of investigating Officers will therefore be lawful for all purposes.

PART B: COVERT HUMAN INTELLIGENCE SOURCES

1. POLICY STATEMENT

In some circumstances it may be necessary for West Dunbartonshire Council employees, in the course of their duties, to conceal their identity by working undercover. Alternatively, there may arise situations when a local authority may covertly ask another person, not employed by the authority, such as a neighbour or an employee (the "source") to obtain information about another person or persons and without that other person's knowledge pass on that information to West Dunbartonshire Council employees. By its nature, actions of this sort may constitute an interference with a 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").

The Regulation of Investigatory Powers (Scotland) Act 2000 provides for the first time a legal framework for the use of such techniques by public authorities (including local authorities) and an independent inspection regime to monitor these activities.

2. OBJECTIVE

The objective of this procedure is to ensure the effective use of Covert Human Intelligence Sources by West Dunbartonshire Council 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 Human Intelligence Sources and any guidance which the Office of the Surveillance Commissioners may issue from time to time.

3. SCOPE OF PROCEDURE

This procedure applies, in all cases, where a Covert Human Intelligence Source is to be used. Covert Human Intelligence Source (hereinafter referred to as a CHIS) is defined by Section 1(7) of RIP(S)A.

A person will be acting as a source if they covertly (ie without disclosing their true purpose) establish or maintain a person or other relationship with a person in order to obtain information from that person or to disclose information obtained from that person or to provide access to information to another person.

The definition of a source is <u>not</u> restricted to obtaining private information.

A local authority may therefore use a source in several ways, for example, employees of West Dunbartonshire Council may, themselves, act as a source by failing to disclose their true identity in order to obtain information. Alternatively, an employee of West Dunbartonshire 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 these instances the person or persons being investigated are unaware that this is taking place.

The procedure may not always apply in circumstances where members of the public volunteer information as part of their normal civic duties or contact members specifically set up to receive anonymous information such as Crime Stoppers. However, someone might become a source as a result of a relationship with West Dunbartonshire Council that began in this way and authorisation must then be sought. It depends on how members of the public have obtained the information. If they have obtained it as an observer they are not a CHIS. If they have obtained it as a result of the existence of a personal or other relationship, they are a CHIS.

Authorising Officers have to be aware of these circumstances.

4. PRINCIPLES OF SURVEILLANCE

In planning and carrying out covert surveillance Council employees have to comply with the following principles. Furthermore, Authorising Officers have to be particularly stringent in detailing the boundaries of the surveillance activity which they, as Authorising Officers, are sanctioning.

Investigating Officers and Authorising Officers should, therefore, ask themselves the following questions when asking/granting authorisation for both Directed Surveillance and a CHIS.

4.1 Is there a lawful purpose?

Covert surveillance shall only be carried out where **necessary** to achieve one or more of the permitted purposes as defined within RIP(S)A. In relation to local authorities, it is for the following reasons:-

(a) For the purpose of preventing or detecting crime or the prevention of disorder.

(b) In the interests of public safety.

(c) For the purpose of protecting public health.

(d) For any other purpose prescribed in an order made by the Scottish Ministers.

4.2 Is the surveillance necessary?

Covert surveillance can only be undertaken where there is no reasonable and effective alternative way of achieving the desired objectives. The question of necessity also has to be viewed in all the circumstances of the specific case before the Authorising Officer.

4.3 Is the surveillance proportionate?

The use and extent of covert surveillance should not be excessive. This means that the surveillance should be proportionate to the significance of what is being investigated. Basically, if the same lawful purpose could be reached by less infringement of a citizen's rights then that lesser path should be taken. When assessing proportionality, employees and Authorising Officers must also consider the seriousness of the alleged behaviour/breach. Minor misdemeanours may not be sufficient to warrant a large surveillance operation. On occasions, sentencing powers in criminal offences may be a useful guide. However, having said that, some regulatory offences can have life threatening consequences, for example, the sale of contaminated foods or dangerous goods and this could result in the surveillance being proportionate. The factors which should be addressed in the decision making process regarding proportionality are whether or not there were relevant and sufficient reasons advanced in support of the application. Was there a less intrusive means of detection/ investigation? Was there procedural fairness in the decision making process and were safeguards against abuse made clear?

When addressing the concept of *proportionality* all Applicants and Authorising Officers should have in mind three basic concepts for consideration.

1. That the use of covert surveillance is a proportionate response to the level of mischief being investigated.

2. That the degree of intrusion upon the target and collaterally is not excessive.

3. That all other reasonable options for gathering the evidence have been considered and rejected.

4.4 Will the proposed surveillance be intrusive?

If the surveillance comes within the definition "intrusive" surveillance in terms of RIP(S)A then no activity can be authorised by any Authorising Officer. As a matter of policy, local authority officers **must not** engage in intrusive surveillance.

4.5 Could there be collateral intrusion?

Reasonable steps should be taken to minimise the possibility that information is obtained on other persons who are not directly involved in the operations. This is also a factor to consider when making the proportionality test.

4.6 Could confidential material be obtained?

Confidential material includes matters subject to legal privilege, for example, this can be information passed between a client and their legal advisor and surveillance should be planned in such a way as to avoid confidential material being obtained. Confidential material should be destroyed once it is no longer necessary for the specific purpose of the surveillance. In particular the proportionality test has to be applied at all times.

5. THE AUTHORISATION PROCESS

Authorisations for the granting of a CHIS follow the same procedure as Directed Surveillance. However, such CHIS authorisations can only be granted if sufficient arrangements have been put in place for handling that source's case. Reference should be made to the Code of Practice. The Code of Practice suggests that applications for the use of conduct of a source will be authorised by Investigations Manager or Head of Service prescribed by the Regulation of Investigatory Powers (Prescription of Officers, Ranks and Positions) (Scotland) Order 2000. The Code of Practice suggests that the designated person for the source should be satisfied of each of the following:-

(a) That there is a responsible officer with day to day responsibility for dealing with the source and for the source's security and welfare;

(b) That there is another officer with general oversight of the use to be made of the source; and

(c) That there is an officer responsible for maintaining a proper record of the use being made of that source, which would include ensuring the security of the record where it may disclose the identity of the source.

In other words, there must be at least two officers with responsibility for dealing with the Human Intelligence Source and the designated person must be satisfied that their duties are properly described and allocated. Best practice would suggest that all these matters should form part of the written records. In such cases for authorisation of a CHIS the application for the use of conduct of a source should be in writing and record:-

- the reasons why the authorisation is necessary in this particular case and on what grounds for example the purpose of preventing or detecting a crime;

- 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, thought has to be given here specifically as to why a CHIS is to be used and why no other means would suffice;

- where a specific investigation or operation is involved, the nature of that investigation or operation;

- the nature of what the source will be tasked to do;

- the details of any potential collateral intrusion and why that 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, the date and time.

Authorisations must be given in writing. In urgent cases only, an Investigations Manager or Head of Service or above may approve oral applications. An application, made in writing, indicating the reasons why an oral authorisation was sought must be made as soon as reasonably practicable. In any case, an oral authorisation will expire after 72 hours. If a source is continued to be used after the 72 hours a further application, in writing, must be made. An oral application is only available where delay would endanger life or jeopardise the investigation.

In accordance with the Code of Practice authorisations will last 12 months. The person responsible for authorising the surveillance must ensure that the authorisation is reviewed at least monthly and those authorisations that are no longer needed or appropriate are cancelled. All reviews must be documented using the Review of Use of Conduct of a Covert Human Intelligence Source Form. Reviews will need to be carried out more frequently where there exists a risk of acquiring confidential material or where the source is a juvenile or deemed vulnerable.

Each department will keep a record of any applications that are refused by the Authorising Officer. Any refusal shall also be recorded in the Central Register.

6. CONFIDENTIAL MATERIAL

Applications where a significant risk of acquiring confidential material has been identified shall always require the approval of the Chief Executive or, in their absence, a Chief Officer.

Confidential material consists of:-

- matters subject to legal privilege, for example, between professional legal adviser and client;

- confidential personal information, for example, relating a person's physical or mental health; or

- confidential journalistic material.

Such applications shall only be granted in exceptional and compelling circumstances where the Authorising Officer is fully satisfied that this conduct is both necessary and proportionate in these circumstances. If granted, such authorisation will last one month. Where any confidential material is obtained then the matter must be reported to the Office of the Surveillance Commissioners during the next inspection and any material obtained made available to them, if requested. Reviews may need to be more regularly carried out than monthly, where the source provides access to confidential material or where collateral intrusion exists.

7. VULNERABLE AND JUVENILE SOURCES AS CHIS

Particular care must be taken where authorising the use or conduct of vulnerable or juvenile individuals to act as sources. The Code of Practice defines a vulnerable individual as "a person who is or may be in need of community care services by reason of mental or other disability, age, illness and who is or may be unable to take care of himself, or unable to protect himself against significant harm or exploitation" (para 4.13). Vulnerable individuals should only be authorised to act as a source in the most exceptional circumstances. Authorisation may only be granted on the approval of the Chief Executive or, in their absence, a Chief Officer. Prior to deciding whether or not to grant such approval the Chief Executive or, in their absence, a Chief Officer, shall seek the advice of the Chief Social Work Officer on the appropriateness of using the individual in question as a CHIS. If granted such authorisation will last one month.

A juvenile is any person under the age of 18. On no occasion should the use of a source under 16 years of age be authorised to give information against his or her parents or any person who has parental responsibilities for him or her. Further, sources under the age of 16 can only give information about other members of their immediate family in exceptional cases.

In other situations authorisation for juveniles to act as a source may only be granted on the approval of the Chief Executive or, in their absence, a Chief Officer and only with the prior advice of the Chief Social Work Officer as described above. The following conditions must also be met:-

- A risk assessment must be undertaken to identify any physical and psychological aspects of their deployment. This risk assessment must be carried out in conjunction with a registered Social Worker from a relevant discipline ie Children and Families, Criminal Justice or Community Care;

- The Authorising Officer must be satisfied that any risks have been properly explained; and

- The Authorising Officer must give particular consideration to the fact that the juvenile is being asked to obtain information from a relative, guardian or other person who has assumed responsibility for their welfare.

An appropriate adult eg Social Worker or Teacher must also be present at any meetings between the authority and a source under 16 years of age.

The maximum authorisation period that can be granted for a juvenile or vulnerable source is one month.

8. DOCUMENTS

This procedure uses the following **documents that shall be used by all departments.**

8.1 Application for Authorisation of the Use or Conduct of a Covert Human Intelligence Source

The Applicant, in all cases, should complete this including where oral authorisation was first sought. It is effective from the time that approval is given.

8.2 Application for Renewal of the Use or Conduct of a Covert Human Intelligence Source

This should be completed where a renewal for authorisation is applied for.

8.3 Review of the Use or Conduct of a Covert Human Intelligence Source

The Authorising Officer shall complete this when carrying out reviews of authorisations.

8.4 Cancellation of the Use or Conduct of a Covert Human Intelligence Source

The Applicant and the Authorising Officer should complete this when the authorisation ceases to be either necessary or appropriate.

9. MANAGEMENT OF SOURCES

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

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

In addition, the Authorising Officer must satisfy themselves that an officer has been designated responsibility for the general oversight of the use made of the source.

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

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

(i) Identity of the source and the means by which the source is referred to;

(ii) The date when and the circumstances when the source was recruited;

(iii) The name of the person with day to day responsibility for the source and the name of the person responsible for overall oversight;

(iv) Any significant information connected with the security and welfare of the source;

(v) Confirmation by the Authorising Officer that the security and welfare of the source have been considered and any risks have been fully explained and understood by the source;

(vi) All contacts between the source and the local authority;

(vii) Any tasks given to the source;

(viii) Any information obtained from the source and how that information was disseminated;

(ix) Any payment, benefit or award or offer of any payment, benefit or award or offer given to a source who is not an employee of the local authority; and

(x) Any relevant investigating authority other than the authority maintaining the records.

10. SECURITY AND RETENTION OF DOCUMENTS AND MATERIALS

Documents created under this procedure are highly confidential and shall be treated as such. Departments shall make proper arrangements for their retention, security and destruction, in accordance with the requirements of the Data Protection Act 2018 and the Code of Practice.

In addition, each department shall also ensure arrangements are in place for the handling, storage and destruction of material obtained through a source in accordance with the requirements of the Data Protection Act 2018 and the Code of Practice.

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

11. CENTRAL REGISTER

A centrally held record of all authorisations is held by the Manager of Legal Services, Municipal Buildings, College Street, Dumbarton G82 1NR. This record is regularly updated whenever an authorisation is granted, renewed or cancelled. The record is retained in a locked cabinet and this record can be made available to the relevant Commissioner or an Inspector from the Office of the Surveillance Commissioners upon request. All records should be retained for a period of at least 3 years from the ending of the authorisation. Furthermore, proper records must be kept of the authorisation and use of a source, detailing all the arrangements in place for ensuring that there is, at all times, a person with responsibility for maintaining a record of the use made of the source until such times as cancellation.

It is recommended that the applicant obtain from Legal Services, before completing an authorisation, next sequential unique reference number prior to completing any authorisation form. This will ensure that in the event of an authorisation being refused, the central record will contain a note of that refusal. This will assist with more effective oversight of processes.

12. OVERSIGHT

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

13. COMPLAINTS

Any member of the public who is unhappy or dissatisfied with the conduct of any covert surveillance, has a right to complain to the Investigatory Powers Tribunal. The individual can also complain through the Council's own Complaints Procedure.

Details of the Complaints Procedure are available for public reference at Legal Services.

The Regulation of Investigatory Powers Act 2000 (the “UK Act”) establishes an independent tribunal. This tribunal has full powers to investigate any complaints and decide any cases within the United Kingdom, including complaints about activities carried out under the provisions of the Regulation of Investigatory Powers (Scotland) Act 2000. Details of the relevant complaint procedure can be obtained from the Investigatory Powers Tribunal, PO Box 33220, London, SW1H 9ZQ.

14. CONCLUSION

In conclusion, RIP(S)A regulates surveillance activity with the aim that the activity will be compliant with the European Convention of Human Rights (ECHR) and that there will be no difficulty in admitting any such evidence as part of a criminal trial.

If the terms of RIP(S)A have been complied with and the dual principles of necessity and proportionality have been addressed, then any interference with any individual’s rights to privacy will be in accordance with the law. The activities and thereafter evidence of investigating Officers will therefore be lawful for all purposes.

PART C: USE OF SOCIAL MEDIA

This part of the Policy address the Council's use of Social Media and highlights were the use of Social Media may require authorisation in terms of RIP(S)A.

Social Media includes but is not limited to Facebook, X, and Instagram.

- Any surveillance (including reviewing Social Media) leading up to the test purchase may require a Directed Surveillance authorisation or a CHIS.

- Cognisance has to be taken regarding the likelihood of private information being obtained.

    - Before an authorisation is required for Directed Surveillance, it must be more likely than not that private information will be obtained

    - Private information can include business information

- We need to consider the individual's expectation of privacy. In particular, a website with access controls will usually mean that the person behind the website has a greater expectation of privacy. Equally, a website with access controls but a very high number of registered users or friends may mean that the person behind the website does not in truth have greater expectations of privacy because they effectively allow anyone to access to their website.

- We need to know if the Officer is using a networked or unnetworked PC. Use of a networked PC may require authorisation, however use of an un-networked PC is more likely to require an authorisation because the surveillance is carried out in a manner that is 'calculated' to ensure that the target is unaware of the surveillance taking place.

- We need to be aware of the frequency and whether or not the surveillance is systematic. Infrequent monitoring to check ongoing compliance is less likely to require authorisation than frequent browsing to gather evidence as part of a specific investigation.

- Collateral intrusion also has to be considered and this is addressed as it is in every authorisation.

It is usually not possible to say with certainty whether any one of those factors on its own will indicate a requirement for an authorisation. Officers must consider all of these issues together and apply them to the unique circumstances of each investigation. Nevertheless, the process can be broken down into approximately three stages depending on the level of intrusion involved:

Stage One

Where there is an open source website where anyone can view information and the website does not apply access controls:

Where there is infrequent browsing to check ongoing compliance, this is unlikely to require a Directed Surveillance authorisation unless an unnetworked PC is used specifically to avoid traceability back to the Council.

Where there is frequent browsing of a website as part of a specific investigation involving the gathering of evidence, then as a rule a Directed Surveillance authorisation should be obtained.

Stage Two

Where a website user has to register by logging in with personal details:

The people behind such websites have a higher expectation of privacy so will usually require a Directed Surveillance authorisation even when the officer logs in using a truthful name and email address. However the people behind websites with a very large number of registered users may have demonstrated that they do not have a high expectation of privacy.

Stage Three

Website where users have to become a “friend”:

A CHIS authorisation should be sought as a ‘relationship’ has been established between the officer and the person behind the website, even if there is no direct communication with the target. This is because the person behind the website should be presumed to give ‘friend’ status only to people that he trusts.

However, the people behind websites with a very large number of ‘friends’ may have demonstrated that they do not have a high expectation of privacy and therefore no ‘relationship’ has in fact been established.

This guidance has been provided to help officers to understand how to apply RIP(S)A to investigations involving social networking websites. It is recognised that there is at present little authoritative guidance from official bodies such as the OSC, Scottish Governments and the courts. The guidance will need to be updated periodically as new information comes to light and as the pattern of trading on the internet evolves.

APPENDIX 1 – LIST OF AUTHORISING OFFICERS

The following Heads of Service are designated Authorising Officers:-

1. Chief Executive confidential material;
2. Service Co-ordinator for Trading Standards;
3. Head of Children's Health and Care and Criminal Justice Service;
4. Chief Officer: Regulatory and Regeneration;
5. Section Head of Litigation and Support or its equivalent; and
6. Service Co-ordinator for Food and Business Group.