Appendix 2

Procedure for Authorisation of the use of Covert Human Intelligence Sources

Contents

1. Foreword

1.1.

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

1.2.

A legal framework ensures that the use, deployment, duration and effectiveness of sources is subject to an authorisation, review and cancellation procedure.

2. Implications of this Procedure

2.1.

In some circumstances, it may be necessary for Orkney Islands Council employees, in the course of their duties, to make use of informants and to conduct 'undercover' operations in a covert manner, i.e. without a person's knowledge. By their nature, actions of this sort may constitute an interference with that person's right to privacy and may give rise to legal challenge as a potential breach of Article 8 of the European Convention on Human Rights and the Human Rights Act 1998 ('the right to respect for private and family life').

2.2.

The Regulation of Investigatory Powers Act (2000) [RIPA] and the Regulation of Investigatory Powers (Scotland) Act (2000) [RIP(S) A] and the Investigatory Powers Act 2016 ('the Acts') together provide a legal framework for covert surveillance activities by public authorities (including local authorities) and an independent inspection regime to monitor these activities.

Deleted: for the first time

2.3.

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

2.4.

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

3. Objective

3.1.

The objective of this procedure is to ensure that all work involving the use or conduct of a source by Orkney Islands Council employees is carried out effectively, while remaining in accordance with the law. It should be read in conjunction with the Regulation of Investigatory Powers (Scotland) Act 2000 and the Scottish Government's Code of Practice on the Use of Covert Human Intelligence Sources ("the Code of Practice").

3.2. Definitions

3.2.1.

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

(a) covertly uses such a relationship to obtain information or to provide information or to provide access to information to another person; or

(b) covertly discloses information obtained by the use of such a relationship or as a consequence of the existence of such a relationship.

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

3.2.2.

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

3.2.3.

Authorising officer is the person who is entitled to give an authorisation for use and conduct of Human Intelligence Source in accordance with section 7 of the Regulation of Investigatory Powers (Scotland) Act 2000.

3.2.4.

Handler means the person referred to in section 7(6) of the Regulation of Investigatory Powers (Scotland) Act 2000 holding an office or position within the local authority and who will have day to day responsibility for:

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

3.2.5.

Controller means the person/the designated managerial officer within the local authority referred to in section 7(6)(b) of the Regulation of Investigatory Powers (Scotland) Act 2000, responsible for the general oversight of the use of the source.

3.2.6.

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

3.2.7.

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

3.2.8.

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

3.2.9.

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

3.2.10.

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

4. Scope of the Procedure

4.1.

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

4.2.

The procedure does not apply to:

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

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

- Particular attention should be made to Social Media Networking Sites. A separate policy is in place in connection with surveillance through social media and should be consulted as necessary. In cases of doubt, the authorisation procedures described below should be followed.

5. Principles of Use or Conduct of Covert Human Intelligence Source

5.1.

In planning and carrying out the source work, Orkney Islands Council employees shall comply with the following principles.

5.2. Lawful purposes

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

5.2.1.

For the purpose of preventing or detecting crime or the prevention of disorder.

5.2.2.

In the interests of public safety.

5.2.3.

For the purpose of protecting public health.

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

It may be necessary to deploy directed surveillance against a potential source as part of the process of assessing their suitability for recruitment, or in planning how best to make the approach to them. An authorisation under this procedure authorising an officer to establish a covert relationship with a potential source could be combined with a directed surveillance authorisation so that both the officer and potential source could be followed.

5.3. Confidential material

5.3.1.

Particular care should be taken with applications where a significant risk of acquiring confidential material has been identified.

5.3.2

Confidential material consists of:

- Matters subject to legal privilege (for example between professional legal advisor and client); special rules apply in relation to directed surveillance carried out on premises where legal consultations are taking place and are referred to in the Procedure for Authorisation of Covert Surveillance.

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

- Confidential journalistic material.

5.4. Vulnerable individuals

5.4.1.

Vulnerable individuals, such as the mentally impaired, will only be authorised to act as a source in the most exceptional circumstances. 5.5 Juvenile sources

5.4.1.

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

5.4.2.

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

5.4.3.

An authorisation for the conduct or use of a source may not be granted or renewed in any case where the source is under the age of 18 at the time of the grant or renewal, unless:

- A person holding an office, rank or position with the relevant investigating authority has made and, in the case of a renewal, updated a risk assessment sufficient to demonstrate that:
    - The nature and magnitude of any risk of physical injury to the source arising in the course of, or as a result of, carrying out the conduct described in the authorisation have been identified and evaluated.
    - The nature and magnitude of any risk of psychological distress to the source arising in the course of, carrying out the conduct described in the authorisation have been identified and evaluated.

- The person granting or renewing the authorisation has considered the risk assessment and is satisfied that any risks identified in it are justified and, if they are, that they have been properly explained to and understood by the source.

- The person granting or renewing the authorisation knows whether the relationship to which the conduct or use would relate is between the source and a relative, guardian or person who has for the time being assumed responsibility for the source's welfare, and, if it is, has given particular consideration to whether the authorisation is justified in the light of that fact.

6. The Authorisation Process

6.1.

Applications for the use or conduct of a source will be authorised by an Executive Director (other than the Executive Director of Corporate Services who has a role of deputising for the Senior Responsible Officer) and in their absence the Head of Legal Services who will give the necessary written authorisation for the use or conduct of the use of Covert Human Intelligence Source. In urgent or exceptional circumstances written or oral authorisation might be given by an officer of Chief Officer grade who has not been designed which should as soon as practicable be followed up by a written authorisation from the relevant official.

6.2.

Authorising officers should ensure that arrangements are in place for the proper oversight and management of sources, including appointing individual officers as defined in section 7(6)(a) and (b) of RIP(S)A for each source as handler and controller. All Officers involved should be suitably trained and experienced.

Deleted: the

Deleted:)

Deleted:

Deleted: ct

6.3.

Authorising officers should not be responsible for authorising their own activities, for example, those in which they, themselves, are to act as the covert human intelligence source or the handler of the covert human intelligence source. Furthermore, authorising officers should, where possible, be independent of the investigation. It is recognised that this is not always possible, especially in the cases of small organisations. However, where possible, clear separation should be maintained between those responsible for the investigation and those managing the covert human intelligence source to ensure that the safety and welfare of the covert human intelligence source are always given due consideration.

6.4.

Deleted: 3

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

6.5.

The case for the authorisation should be presented in the application in a fair and balanced way. In particular, all reasonable efforts should be made to take account of information which supports or weakens the case for the authorisation.

6.6.

Deleted: 4

All applications for covert human intelligence source renewals will be made on form OIC/ren/chis. The applicant in all cases should complete this where the source work

requires to continue beyond the previously authorised period (including previous renewals). The renewal of the authorisation should be signed by the authorising officer.

6.7. Deleted: 5

Where authorisation ceases to be either necessary or appropriate the authorising officer and the applicant will cancel an authorisation using form OIC/can.chis.

6.8. Deleted: 6

Forms, codes or practice and supplementary material will be available from the Council Intranet.

6.9. Deleted: 7

Any person giving an authorisation for the use of a covert human intelligence source must be satisfied that:

- Account has been taken of the likely degree of intrusion into the privacy of persons other than those directly implicated in the operation or investigation ('collateral intrusion'). Measures must be taken, wherever practicable, to avoid unnecessary intrusion into the lives of those affected by collateral intrusion. Particular consideration should be given in cases where religious, medical, journalistic or legally privileged material may be involved, or where the communications of a member of a relevant legislature may be involved.
- The authorisation is necessary (see below).
- The authorised surveillance is proportionate (see below).
- Satisfactory arrangements exist for the management of the source.
- In particular when Environmental Health Investigators deploy DAT noise level monitors to assist in any enforcement action in relation to noisy neighbour complaints. These cases should be reviewed on a case by case basis and if necessary the appropriate authorisation sought.

6.10. Deleted: 8

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

6.10.1. Deleted: 8

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

6.10.2.

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

6.10.3.

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

6.10.4.

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

6.10.5.

The records maintained by Orkney Islands Council that discloses the identity of the source will not be available to persons except to the extent that there is a need for access to them to be made available to those persons. The records kept by Orkney Islands Council should be maintained in such a way as to preserve the confidentiality of the source and the information provided by that source. There should, at all times, be a designated person within the authority who will have responsibility for maintaining a record of the use made of the source.

6.11.Necessity

An authorisation for the use of a Covert Human Intelligence source is necessary on grounds falling within section 7 (3) of RIP(S)A if it is necessary-(a) for the purpose of preventing or detecting crime or of preventing disorder; (b) in the interests of public safety; or (c) for the purpose of protecting public health.

6.12. Effectiveness

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

6.13. Proportionality

The use of covert human intelligence sources must be proportionate or in terms of RIP(S)A section 7(b) that the authorised conduct or use is proportionate to what is sought to be achieved by that conduct or use

A potential model answer would make clear that the following 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.

- Whether there are any implications of the authorised conduct for the privacy of others, and an explanation of why (if relevant) it is nevertheless proportionate to proceed with the operation.

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

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

The degree of intrusiveness of an authorisation of a covert human intelligence source will vary from case to case, and therefore proportionality must be assessed on an individual basis.

6.14. Authorisation

Deleted: 2

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

The authorising officer must take into account the following issues when considering an application:

- who is to be deployed as the source.
- what is being proposed.
- where and when the proposed deployment will take place.
- whether it is necessary and proportionate.

6.14.1.

However, the tasking of a person should not be used as the sole benchmark in seeking an authorisation. It is the activity of the covert human intelligence source in exploiting a relationship for a covert purpose which is ultimately authorised by RIP(S)A, whether or not that source is asked to do so by the Council. It is possible therefore that a person will become engaged in the conduct of a covert human intelligence source without the Council inducing, asking or assisting the person to engage in that conduct. An authorisation should be considered, for example, where the Council is aware that a third party is independently maintaining a relationship (i.e. self-tasking) in order to obtain evidence of criminal activity, and the Council intends to make use of that material for its own investigative purposes.

6.14.2.

Underlying all of these considerations is the requirement for the authorising officer to be satisfied that the terms of the legislation and relevant guidance are met.

6.14.3.

The authorising officer should clearly complete the “Authorising Officer’s Statement” on the application form, preferably in their own hand, and articulate in their own words what activity they are authorising.

The Authorising Officer must state explicitly what is being authorised

6.14.4.

The Authorising Officer must 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. The Authorising Officer should specify the details of how and why they consider the application to be both necessary and proportionate.

Authorisation different from application

6.14.5.

If an application fails to include an element in the proposed activity which in the opinion of the Authorising Officer should have been included (for example, the return of something to the place from which it is to be taken for some specified activity), or which is subsequently requested orally by the applicant, it may be included in the authorisation; if so, a note should be added explaining why. Conversely, if an Authorising Officer does not authorise all that was requested, a note should be added explaining why. This requirement applies equally to intrusive surveillance, property interference, directed surveillance and CHIS authorisations.

6.14.6.

It is important to note that the reactive nature of the work of a covert human intelligence source, and the need for him/her to maintain cover, may make it necessary for the source to engage in conduct which was not envisaged at the time the authorisation was granted, but which is incidental to that conduct. Such incidental conduct is regarded as properly authorised by virtue of sections 1(6)(a), 5 and 7(5) of RIP(S)A, even though it was not specified in the initial authorisation.

The Senior Responsible Officer should avoid granting authorisations

6.14.7.

The role of the Senior Responsible Officer is to oversee the competence of Authorising Officers and the processes in use in their public authority. Whilst legislation does not preclude their use as an Authorising Officer, it is unlikely that they would be regarded as objective if they oversee their own authorisations.

6.14.8. Deleted: 3

Additionally, the authorising officer must assess risks to a source in carrying out the conduct in the proposed authorisation. The risk assessment must be made by the applicant and presented to the authorising officer for consideration. A risk assessment is carried out to determine the risk to the source of any tasking and the likely consequences should the role of the source become known. The ongoing security and welfare of the source, after the cancellation of the authorisation, will also be considered from the outset.

Use of a covert human intelligence source with technical equipment

6.1.9

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

6.14.10

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

7. Security and Welfare

The Council, when deploying a covert human intelligence source, should take into account the safety and welfare of that source when carrying out actions in relation to an authorisation or tasking, and the foreseeable consequences to others of that tasking. Before authorising the use or conduct of a covert human intelligence source, the authorising officer should ensure that a risk assessment is carried out to determine the risk to the source of any tasking and the likely consequences should the role of the source become known. This should consider the risks relating to the specific tasking and circumstances of each authorisation separately, and should be updated to reflect developments during the course of the deployment, as well as after the deployment if contact is maintained.

8. Time Periods – Authorisations

8.1.

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

8.2.

In terms of the Scottish Government's Code of Practice a written authorisation granted by an authorising officer will cease to have effect (unless renewed) at the end of a period of twelve months beginning with the day on which it took effect. Authorisations for the deployment of a juvenile source are for one month.

9. Time Periods – Renewals

9.1.

Before an authorising officer renews an authorisation, they must be satisfied that a review has been carried out of the use of a source as outlined in paragraph 10.1.

Deleted: 4

Deleted: 7

Deleted: 7

Deleted: 7

Deleted: 8

Deleted: 8

Deleted: 9

9.2.

If at any time before an authorisation would cease to have effect, the authorising officer considers it necessary for the authorisation to continue for the purpose for which it was given, they may renew it in writing for a further period of twelve months. Renewals may also be granted orally in urgent cases and last for a period of seventy two hours.

9.3.

A renewal takes effect at the time at which, or day on which the authorisation would have ceased to have effect but for the renewal. An application for renewal should not be made until shortly before the authorisation period is drawing to an end. Any person who would be entitled to grant a new authorisation can renew an authorisation. Authorisations may be renewed more than once, in necessary, provided they continue to meet the criteria for authorisation. The renewal should be kept/recorded as part of the authorisation record.

9.4.

Authorisations for the deployment of a juvenile source are renewable for a further period or further periods of one month each.

10. Review

10.1.

The Authorising Officer shall keep all authorisations under constant review and an authorisation will be cancelled immediately the requirement for surveillance ceases. The Authorising Officer should set review dates and ensure that all reviews are carried out immediately after the source has been deployed with the review period tailored to meet the particular requirements of the investigation. Details of the review and the decision reached shall be noted on the Review Form.

10.2.

Particular attention should be given to the need to review authorisations frequently where they involve a high level of intrusion into private life or significant collateral intrusion, or particularly sensitive information is likely to be obtained. At the point when the Council is considering applying for an authorisation, it must have regard to whether the level of protection to be applied in relation to information obtained under the warrant or authorisation is higher because of the particular sensitivity of that information.

10.3.

In each case, unless specified by a Judicial Commissioner, the frequency of reviews should be determined by the Council. This should be as frequently as is considered necessary and proportionate.

10.4.

In the event that there are any significant and substantive changes to the nature of the operation during the currency of the authorisation, the Council should consider whether it is necessary to apply for a new authorisation.11.

Cancellation

11.1.

The authorising officer and the applicant must keep each authorisation under review. The applicant must notify the authorising officer if they consider that the authorisation is no longer necessary or proportionate. The authorising officer must cancel an authorisation if they are satisfied that the use or conduct of the source no longer satisfies the criteria for authorisation or that procedures for the management of the source are no longer in place. Where possible, the source must be informed that the authorisation has been cancelled.

11.2.

Where necessary and practicable, the safety and welfare of the covert human intelligence source should continue to be taken into account after the authorisation has been cancelled and risk assessments maintained. The authorising officer will wish to satisfy himself/herself that all welfare matters are addressed and should make appropriate comment in their written commentary.

12. Record Keeping

12.1.

Each Service or discrete location within Services must maintain a record of all applications for authorisation (including refusals), renewals, reviews and cancellations. A centrally retrievable record of all authorisations will be held by Legal Services and regularly updated whenever an authorisation is granted, renewed or cancelled. An application for authorisation cannot proceed until a unique reference number (URN) has been issued by Legal Services and Legal Services must have sight of each and every application. The central register shall be kept up-to-date all times. 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 at least five years. The Council's Policy for Authorisation on use of Covert Human Intelligence Sources contains further details at Paragraph 8 thereof.

12.2.

In addition consideration should be given to maintaining auditable records for individuals providing intelligence who do not meet the definition of a covert human intelligence source. This will assist the Council to monitor the status of an individual and identify whether that person should be duly authorised as a covert human intelligence source. This should be updated regularly to explain why authorisation is not considered necessary.

Deleted: ¶
Deleted: 0
Deleted: 0
Deleted: 1
Deleted: 1
Deleted: Commissioner or an
Deleted: Office of Surveillance
Deleted: ers
Deleted: three
Deleted: Orkney Islands

13. Security and Retention of Documents

13.1.

Documents created under this procedure are highly confidential and shall be treated as such. Services shall make proper arrangements for their retention, security and destruction, in accordance with the requirements of all relevant data protection legislation, Chapter 8 of the Code of Practice and any Code of Practice produced by Orkney Islands Council.

13.2.

Legal Services will maintain the Central Register of Authorisations. Authorising officers shall notify the Legal Services of the grant, renewal or cancellation of any authorisations and the name of the Applicant Officer within 1 working day to ensure the accuracy of the Central Register.

13.3.

The Authorising Officer shall retain the original Authorisation and Renewal Forms until cancelled. On cancellation, the original Application, Renewal and Cancellation forms shall be forwarded to the Legal Services with the Authorising Officer retaining a copy.

13.4.

The Authorising Officer shall retain the copy forms for at least one year after cancellation. Legal Services will retain the original forms for at least five years after cancellation. In both cases these will not be destroyed without the authority of the authorising officer if practicable.

13.5.

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

14. Particulars to be Contained in Records

(a) the identity 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.

Deleted: 2

Deleted: 2

Deleted: the

Deleted: D

Deleted: P

Deleted: Act 1998

Deleted: and

Deleted: 2

Deleted: 2

Deleted: 2

Deleted: 2

Deleted: 3

(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.

(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.

(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.

15. Oversight

The Investigatory Powers Act 2016 establishes an Investigatory Powers Commission to provide comprehensive oversight of the use of the powers to which this Procedure applies. This oversight includes inspection visits by Inspectors appointed by the Investigatory Powers Commission.

Deleted: Office of Surveillance Commissioners (OSC) provides independent oversight of the use of the powers contained within the Regulation of Investigatory Powers (Scotland) Act 2000

Deleted: OSC

16. Complaints

Deleted: 5

The Investigatory Powers Tribunal has jurisdiction to investigate and determine complaints against public authority use of investigatory powers. Any complaints in respect of the use by the Council of its powers described in this Procedure should be directed to the Investigatory Powers Tribunal. Full details of how to present a complaint are available on the Tribunal's website – www.ipt-uk.com.

Deleted: Regulation of Investigatory Powers Act 2000 (the UK Act) establishes an independent Tribunal. This has full powers to investigate and decide any cases within its jurisdiction. A leaflet titled 'Investigatory Powers Tribunal: Regulation of Investigatory Powers Act 2000' sets out the complaints procedure. This is available from the Council Intranet and includes a form for a person to complain to the Tribunal.