Aberdeen City Council- Corporate Protocol and Procedure on Covert Surveillance[1]

Contents

Appendices:

[1] **Issue 4 (July 2020)**

1. Introduction

1.1 This Protocol provides an overview of the arrangements Aberdeen City Council (ACC) has in place to manage occasions on which it is necessary for Officers to undertake covert surveillance, either via Directed Surveillance (DS) or through the use of a Covert Human Intelligence Source (CHIS).

1.2 This Protocol and Procedure document should be used in conjunction with the Scottish Government "Covert Surveillance and Property Interference Code of Practice", the Scottish Government "Covert Human Intelligence Sources Code of Practice" and the Office of the Surveillance Commissioners (OSC) "Covert Surveillance and Property Interference, December 2017". All three publications are available on the Covert Surveillance page of the Intranet or on the Khub.

1.3 This Protocol and Procedure is reviewed annually, and any changes are reported to the Audit Risk and Scrutiny Committee as part of the Annual Report. Any amendments to the Protocol and Procedures shall be approved in accordance with the General Powers to Chief Officers as set out in the Council's Powers Delegated to Officers.

1.4 The Council does not access communications data under the Regulation of Investigatory Powers Act 2000 and as such is not registered with the National Anti-Fraud Network to use their services.

2. Overview of Legislative Position

2.1 There are a range of situations in which the Council's employees, in the course of their duties, have to carry out investigations and activities which, by their very nature are **covert**, i.e. they are concealed, secret or clandestine.

2.2 Under the Human Rights Act 1998 ('HRA 1998') it is unlawful for a public authority to act in a way which is incompatible with a European Convention on Human Rights ('ECHR') right.

2.3 In accordance with the HRA 1998, it is essential that covert investigations are compatible with Article 8 of ECHR which states that: "*everyone has the right to respect for his private and family life, his home and correspondence".*

2.4 The rights guaranteed in Article 8 can be interfered with if such action can be justified as being in accordance with the law and necessary in the interests of at least one of the following:

- national security;
- public safety;
- the economic well-being of the country;
- the prevention of disorder or crime;
- the protection of health or morals; or
- the protection of the rights and freedoms of others.

2.5 The Regulation of Investigatory Powers (Scotland) Act 2000 ("RIPSA") came into force on 29th September 2000 and is applicable in Scotland only. It provides a legal framework for covert surveillance by public authorities and an independent inspection regime to monitor these activities. RIPSA sets out a process for the authorisation of covert surveillance by designated officers, for the duration of that authorisation and for the review, termination or renewal of authorisations.

2.6 The primary purpose of RIPSA is to ensure compliance with Article 8 in relation to covert surveillance. As such, so long as local authority investigators, acting in the course of their duties, ensure that they obtain an authorisation **and** that they act in accordance with that authorisation, any interference with Article 8 rights will be in accordance with the law and therefore the activities and evidence of investigating officers will be lawful.

3. Definitions

3.1 Surveillance includes:

- Monitoring, observing or listening to persons, their movements, their conversations or their other activities or communications.
- Recording anything that is monitored, observed or listened to in the course of surveillance.
- Surveillance by, or with, the assistance of a surveillance device

3.2 Surveillance can be overt or covert.

- Overt: Surveillance is overt where it is carried out in such a way that anyone subject to it is aware that the surveillance is taking place.

  Examples:

  - CCTV cameras recording a general scene. Members of the public should be aware of such use by notices placed in the area.
  - City Wardens observations in the Community as their presence will be obvious due to their uniforms.

- Covert Surveillance is covert where it is carried out in such a way that anyone subject to it is unaware that the surveillance is taking place.

  Examples:

  - External Agency requesting access to Council CCTV system to undertake a specific investigation
  - Covert video recording of Trading Standards test purchasing
  - Covert monitoring of Social Media Profile(s) of a client / customer

3.3 RIPSA only applies to **covert surveillance** – no authorisation is necessary for overt surveillance. Officers who are unsure if the surveillance they plan to conduct is overt or covert should seek advice from the Regulatory & Compliance Team, Legal Services prior to undertaking the surveillance.

3.4 There may be situations where covert surveillance is desired but the requirements of RIPSA cannot be met. In these cases, legal advice **MUST** always be sought prior to any action being taken, as an assessment of the nature of the issue, need for covert surveillance, risks/ mitigations associated with undertaking surveillance and privacy implications need to be addressed. In *BA and others v Chief Constable of Cleveland Police*[2], Cleveland Police (CP) placed a covert camera in a resident's flat to capture evidence that the resident's carers were stealing items from her. The authorisation of the use of such a camera did not fall within the definition of "intrusive surveillance" as the crime alleged was not "serious". Instead, CP undertook a similar approach to assess the privacy implications, risks, and mitigations of using a covert

[2] IPT/11/129/CH; IPT/11/133/CH & IPT/12/72/CH

camera and authorised the conduct, albeit not under RIPA. Because there was proper consideration of whether an authorisation should be sought and this was evident, the Tribunal was satisfied that although the conduct was not protected by a surveillance authorisation, there was no unlawful activity or a breach of Article 8 of the Human Rights Act 1998.

3.5 Covert Surveillance should only be undertaken by suitably trained or experienced employees and consideration must be given to employees' health & safety at all times.

3.6 There are three types of covert surveillance, only two of which Aberdeen City Council can conduct:

- **Directed Surveillance** (DS)
    - Surveillance which is covert but not intrusive and undertaken:
        - For the purposes of a specific investigation or specific operation

          and

        - In such a manner as is likely to result in the obtaining of private information about any person.

          Private information includes information relating to the person's private or family life, or personal relationships with others, including professional or business relationships.

- **Covert Human Intelligence Source** (CHIS) (See section 6 for further guidance)
    - A CHIS establishes or maintains a false personal relationship with others to obtain or access information covertly
    - Covers some 'undercover work' undertaken by local authorities where the officer (without disclosing his or her true identity) pursues an investigation by dealing with a particular individual gaining their confidence with a view to securing information
    - May also apply to situations where a Council Officer a) receives information from someone who approaches them voluntarily on repeated occasions or b) asks an individual to use a relationship they already have to gain information about a person of interest.

- **Intrusive Surveillance**

    - Covert surveillance carried out in relation to anything taking place on any residential premises or in any private vehicle which involves the presence of an individual on the premises or in the vehicle or is carried out by means of a surveillance device.

    - No provision within RIPSA for a local authority to conduct intrusive surveillance, only a Chief Constable can authorise such surveillance being undertaken.

    - As such, Local Authority Officers **MUST NOT** engage in intrusive surveillance

4. Key Principles

4.1 In order to be lawful, covert surveillance must:

- Have a **lawful purpose** which directly relates to Aberdeen City Council's regulatory (core) functions and be in pursuance of one of the following:

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

    - In the interests of public safety

    - For the purposes of protecting public health

    - For any other purpose prescribed in an order made by the Scottish Ministers.

- Be **necessary**

    - Covert surveillance can only be undertaken where there is no reasonable and effective alternative way of achieving the desired objectives.

    - Necessity must be viewed in all of the circumstances of the specific case

- Be **proportionate**

- The use and extent of covert surveillance should not be excessive and should be proportionate to the significance of what is being investigated.

- If the same information could be gathered by less infringement of a citizen's rights, then the lesser path should be taken.

- In considering proportionality, consideration should be given to the seriousness of the alleged behaviour / breach

4.2 In addition, surveillance should be planned in such a way as to avoid any confidential material, such as matters subject to legal privilege, confidential medical information or confidential journalistic material, from being obtained and applications where there is a significant risk of acquiring confidential material require to be authorised by the Chief Executive or, in her absence, the Director who is deputising for her as Head of Paid Service.

5. Training

5.1 Aberdeen City Council has a RISPA Training Policy. This identifies a process whereby each job role within the authority is tiered as applicable to the role's exposure to Covert Surveillance activities. For those in Tiers 2 and 3, awareness raising on risk assessments and potential surveillance situations is carried out as and when required.

5.2 Any officer of the Council who wishes to make an application for an authorisation for Covert Surveillance **MUST** have undertaken training prior to applying for, and conducting, covert surveillance.

5.3 Training is delivered on request. Please contact the Team Leader, Regulatory & Compliance, Legal Services to request and arrange training.

5.4 Awareness raising is an important part of RIPSA compliance. All applicants and Authorising Officers who have attended mandatory training are invited to be a member of a restricted forum which is managed and supported by the Regulatory & Compliance Team, Legal Services. This Protocol, the procedures and guidance on all aspects of RIPSA, updates on new case law, feedback from audits of application forms and links to committee reports are available on the forum. It also provides an opportunity for applicants to raise matters relating to RIPSA activity in a more interactive way.

6. Covert Human Intelligence Source (CHIS)

6.1 Where an employee establishes or maintains a relationship with a view to obtaining or accessing information covertly, a CHIS Authorisation is necessary. This includes situations where, without disclosing his or her true identity, an officer pursues an investigation by dealing with a particular individual over a prolonged period thereby gaining this confidence with a view to securing information.

6.2 In addition, a CHIS can be a person who supplies information to a Council employee on a purely voluntary basis where it has not been sought out by the authority. If the information being provided is recorded as potentially useful or actionable, the Council has a duty of care to the individual and, in order to manage this source appropriately, an authorisation may be necessary. In situations where the Council is receiving information from a voluntary source, particularly attention must be given to paragraphs 2,17; 2,18 and 2.23 – 2.25 of the Scottish Government "Covert Human Intelligence Sources Code of Practices".

E.g. *Where a person is asked to maintain a record of all vehicles arriving and leaving a specific location or to record the details of visitors to a neighbouring house. A relationship has not been established or maintained in order to gather the information and a CHIS authorisation is not available though there may be a need for a Directed Surveillance authorisation. Where an officer of the Council has asked a person to use their existing relationship with a person of interest to the Council, to illicit information from that person for the Council's purpose, that conduct would require a CHIS authorisation and this should be discussed with Legal Services in the first instance*.

For further guidance, please see the Guidance Note: Identifying a CHIS on Khub or the Intranet.

6.3 There are a number of groups to which special consideration must be given prior to their use as a CHIS:

- Juvenile: Juvenile source are those under the age of 18. The maximum duration of authorisation for juvenile sources is one month as opposed to the usual 12month duration for adult sources. Where you are considering the use of a Juvenile, please contact the Regulatory & Compliance Team, Legal Services, for advice prior to seeking an authorisation.

- Vulnerable Individuals: A vulnerable individual is a person who may be in need of community care services by reason of mental or other disability, age or illness **and** who is or may be unable to take care of himself, or be unable to protect himself from significant harm of exploitation. Only in the most exceptional of circumstances should vulnerable individual be authorised as a source.

Only the Chief Executive, or in her absence the Director deputising for her as Head of Paid Service, can authorise an application to authorise the use of juveniles or vulnerable individuals as a source.

6.4 Authorisation for the use of a Covert Human Intelligence Source (CHIS) can only be granted if sufficient arrangements are in place for handling the Source. Those arrangements are:

- That a suitably trained and / or experienced Officer is appointed as the Handler of the Source. The Handler is responsible for dealing with the CHIS on behalf of the Council; directing the day to day activities of the CHIS; recording information supplied by the CHIS and monitoring the CHIS's security and welfare.

- That a suitably senior Officer, normally the Handler's Line Manager, is appointed as the Controller of the Source. The Controller is responsible for the supervision of the Handler and for general oversight of the use of the CHIS.

- That the Authorising Officer is satisfied that suitable arrangements are in place for maintaining a record of the use made of the source including:

    - The identity of the Source and the identity used by the Source in the operation
    - The detail of any other relevant investigating authority involved
    - The means by which the Source is referred to in each investigating authority
    - Any other significant information connected with the security and welfare of the source and confirmation these have been properly explained to and understood by the Source
    - The date when, and the circumstances in which the Source was recruited
    - The identities of the Handler, Controller and Authorising Officers and the period(s) in which these people have discharged their responsibilities
    - All contacts / communications between the Source and the Handler
    - Information obtained through the conduct on use of the Source and any dissemination of that information.

7. Application Process

7.1 Prior to any application being made, the Applicant must contact the Team Leader, Regulatory & Compliance, Legal Services (Ext: 522553, or 523168) to request a Unique Application Reference Number which will apply to the Application and Authorisation. This number must be inserted on each page of the Application/ Authorisation form.

7.2 Before any specific covert surveillance is undertaken, the relevant officer (Applicant) requires to complete a "Part 1- Directed Surveillance Application Form" or a "Part 1- CHIS Application Form", print and sign the application and submit it in hard copy to an Authorising Officer for consideration[3]. These application forms can be downloaded from the RIPSA page on the Intranet or Khub. No Covert Surveillance can be undertaken prior to a specific authorisation being granted.

7.3 The role of the Applicant is to present the facts to the Authorising Officer. Facts must include:

- The **issue** being investigated;
- **Why** the investigation has to be covert;
- **What** covert surveillance is requested and why;
- **Where** and **When** the covert surveillance will take place;
- **Who** the covert surveillance will focus on;
- **Who** else may be affected by the covert surveillance;
- **How** it is intended to conduct the covert surveillance.

Further, for an application for the authorisation of a use of a CHIS, the following additional information is also required:

- The **identity** of the CHIS, the Controller and the Handler.
- Details of the risk assessment undertaken on the **security** and **welfare** of using the source.

In addition, the completed Application Form must provide sufficient detail to allow the following points to be considered:

- Necessity
    - The application must state which of the four purposes outlined in paragraph 4.1 above apply.

[3] Where applicants are working remotely and not able to produce a hard copy Application form, they should apply a wet signature to Part 1 and convert it to a PDF document before sending it to an Authorising Officer for authorisation.

- In addition, specific detail of which legislative provision(s) apply, and/or which powers the Council is seeking to utilise, should be detailed, including the power delegated to that officer by their respective Director, as set out in the Powers Delegated to Officers which forms part of the Council's Scheme of Governance.
- The application must detail why the application is necessary at the time it is made, it is not appropriate to seek authorisation for activities that may be necessary at some point in the future.

- Effectiveness
  - The application must detail how the covert surveillance will be undertaken and who will do it, the time period(s) and date(s) when it will be done, and the location. It can be useful to provide a map or illustration of the site in order to demonstrate to the Authorising Officer the sight lines and why the location chosen is suitable for the intended operation.
  - If a device is being used, it is important to set out in the application form, what the device is and how the data collected on the device is managed, maintained and preserved for evidential purposes.[4]

- Collateral Intrusion
  - The application must demonstrate that account has been taken of the likely nature and degree of intrusion into the privacy of persons other than the intended target of the investigation.
  - The application must detail what measures will be taken to avoid unnecessary intrusion into the lives of others. It is necessary that all reasonable practicable measures are implemented.
  - Consideration should also be given to any particular sensitivities in the local community where the surveillance is being conducted and of any similar activities being undertaken by other public authorities which could have an impact on the operation. It is advisable that the applicant should make the local policing team aware that surveillance will be carried out at a certain location, should that be authorised, ahead of the operation starting.

[4] Please refer to the Guidance Note: Management of a Surveillance Device which is available on the Intranet and Khub.

- Proportionality
    - The application should outline the following factors for the Authorising Officers consideration:
        - The balance of the size and scope of the operation against the gravity and extent of the perceived mischief
        - How and why the methods proposed will cause the least possible intrusion on the target and other people
        - That the covert surveillance activity proposed is the only reasonable way, having considered any other possible ways, of obtaining the desired result

Further guidance on proportionality is set out in a Guidance Note on Proportionality which is contained in Appendix One of this protocol and is also available on the Intranet or Khub.

A guide on completing the application form is contained in Appendix Four of this protocol.

7.4 Upon completion, the application form is passed to one of the Council's Authorising Officers.

8. Authorising Officers

8.1 An Authorising Officer is a person who is entitled to give an authorisation for covert surveillance in accordance with the applicable regulations. No other officer, with the exception of that outlined in paragraph 8.4 below, is able to authorise covert surveillance to take place. A current list of Authorising Officers is available on the Covert Surveillance pages on the Intranet and Khub.

8.2 It is the responsibility of the Authorising Officer to assess and approve the necessity and proportionality of any proposed covert surveillance activity.

8.3 Authorising Officers are appointed by the Chief Officer- Governance and once trained, their contact details uploaded to the Intranet and Khub.

8.4 In addition, and as stated in paragraph 4.2 above, if there is a significant risk of confidential material (for example matters subject to legal privilege, confidential medical information or confidential journalistic material) being acquired during the covert surveillance, the application requires to be authorised by the Chief Executive or, in her absence, by the Director who is deputising for her as Head of Paid Service.

9. Authorising Process

9.1 Authorising Officers should avoid authorising activities / operations for which they have responsibility wherever possible and should only do so in exceptional circumstances.

9.2 Prior to authorising the use of Directed Surveillance or a CHIS, Authorising Officers must satisfy themselves that:

- The application form has been completed correctly and that it addresses all the requirements of RIPSA and the Code of Practice on Covert Surveillance and Property Interference and/or the Code of Practice on the Use of a Covert Human Intelligence Source.
- The application is for one of the lawful purposes set out in the Act
- All of the required considerations have been addressed adequately.

9.3 Where there is insufficient evidence within the application to enable the Authorising Officer to adequately consider the use of directed surveillance or a CHIS, the Authorising Officer should be prepared to challenge the content of the application form and refuse or limit the extent of authorisation.

9.4 Authorising Officers must also consider the health and safety of the staff involved prior to giving authorisation, in line with current Council policies and procedures. For this purpose, when completing the application, a risk assessment must be carried out and recorded on the application form. The risk assessment must determine the risk to the source of the tasking proposed, the members of staff involved in the surveillance, the likely consequences should the role of the source become known and the on-going security and welfare of the source both during the authorisation and following the cancellation of the authorisation.

9.5 Authorising Officers determine whether to approve or refuse the application for covert surveillance. If the application is approved, the Authorising Officer must in addition to 9.4, detail in Part 2- The Authorisation Form:

- A description of the covert surveillance activity authorised
- Detail of the exact extent of the covert conduct authorised including the time period(s) in which it will take place and the location(s) where it will be conducted. The “5 W’s” – **Who**, **What**, **Where**, **When** and **How** – must be detailed clearly in the application.

This may not always accord with the full extent of the application and will depend on circumstances.

9.6 It is **essential** that all original paperwork be forwarded by Authorising Officers to the Regulatory & Compliance Team, Legal Services who maintain the Central Record of all Directed Surveillance and CHIS Applications and Authorisations. The Authorising Officer must forward the original Part 1- Application and Part 2- Authorisation to the Central Record. Copies can be retained by the Service but should be destroyed in accordance with their own Retention policies.

9.7 Where it is in the overriding public interest to secure information by covert surveillance as a matter of urgency, when it would not be practicable to do anything other than act immediately, urgent authorisation can be grated verbally. Such authorisation can last for a maximum of 72 hours and must be recorded in writing as soon as reasonably practicable.

9.8 Where the Authorising Officer decides to refuse the application, he/ she must record their reasons for refusal within Part 2- the Authorisation.

10. Authorisation Review and Cancellation

10.1 Each written authorisation for Directed Surveillance expires **3 months** after the date on which it was granted. A written authorisation for a CHIS expires **12** months after the date on which it was granted. At any time before an authorisation expires, it can be **extended** (renewed) for a further 3 month period, subject to an Authorising Officer agreeing that such an extension (renewal) is necessary. Appendix 6 sets out the process for Reviews, Renewals or Cancellations.

10.2 In addition, each authorised covert surveillance operation must be **reviewed** at intervals of not more than one month by the Authorising Officer who authorised the application. Any changes in circumstances must be considered. The review may lead to the authorisation being continued, the authorisation being varied or the authorisation being cancelled. Where it is not reasonably practicable for the same Authorising Officer to undertake the review (i.e they are on holiday, out of the country, or have left employment with Aberdeen City Council), the review can be undertaken by another Authorising Officer. At the Review meeting, the Authorising Officer must have regard to any information obtained in the initial operation, whether there are legitimate grounds to renew or vary the authorisation and be satisfied that the operation still remains necessary and proportionate, set out clearly the new terms of his/ her authorisation or, where of the view that the operation is complete or no longer necessary, to order it be cancelled.

10.3 The Authorising Officer who granted or last renewed the authorisation must **cancel** an authorisation if he/she is satisfied that the Directed Surveillance operation/ CHIS is no longer necessary or proportionate. The cancellation should occur as soon as possible. Where it is not reasonably practicable for the same Authorising Officer to undertake the cancellation (i.e they are on holiday, out of the country, or have left

employment with Aberdeen City Council), the cancellation can be made by another Authorising Officer. The Authorising Officer should be clear about the outcome of the operation, how the evidence obtained is being preserved (see 11.2.2 below) and whether or not the objectives of the operation were achieved.

10.4 All original paperwork for an application, review, renewal or cancellation must be forwarded by the Authorising Officer to the Regulatory & Compliance Team, Legal Services for retention in the Central Record. Part 1- Application Form and Part 2- Authorisation Form should be sent to the Central Record after the operation had been authorised. The original paperwork for a Review, Renewal or Cancellation should be sent to the Central Record after the surveillance operation is complete. As stated at section 11 below, documents within the Central Record are highly confidential and will be stored, retained and destroyed within the requirements of the Data Protection Act 2018 and any relevant retention policy of the Council.

11. Safeguarding, Monitoring and Quality Control

11.1.1 Each Service or discrete location within a Service must maintain its own record of all applications made for authorisation, including instances where an application has been refused, renewed, reviewed and cancelled. This record must be kept in a secure, locked location where access to those records are restricted to persons who have a legitimate purpose to access the information. Separate files should be maintained in respect of the authorisation of Directed Surveillance and the authorisation of Covert Human Intelligence Sources.

11.1.2 If records of RIPSA applications/ authorisations are kept electronically, access to the electronic record must be secure and restricted to persons who have a legitimate purpose to access the information.

11.1.3 All original paperwork and operational practice will be reviewed by the Regulatory & Compliance Team, Legal Services. The purpose of these reviews will be to identify any areas of procedural or policy weakness, good practice and to assess future training requirements. If necessary, Applicants and Authorising Officers may be contacted as part of this review and learning points from each will be addressed via appropriately formatted briefings.

11.1.4 Dissemination, copying[5] and retention of material must be limited to the minimum necessary for authorised purposes. In accordance with the Code of Practice[6], something is necessary if the material;

- is, or is likely to become, necessary for any of the statutory purposes set out in RIPSA or the 1997 Act[7] in relation to covert surveillance;
- is necessary for facilitating the carrying out of functions of public authorities under those Acts;
- is necessary for facilitating the carrying out of any functions of the IPC of the IPT[8];
- is necessary for the purposes of legal proceedings; or
- is necessary for the performance of any functions of any person or under any enactment.

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

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

12. Oversight of Covert Surveillance Arrangements

12.1 The Investigatory Powers Commissioner (IPC) provides independent oversight of the use of powers contains within RIPSA.

---

[5] Copying includes extracts and summaries which identify themselves as being a product of the surveillance/ any record which refers to the surveillance and the identities of the person who whom the material relates.
[6] Scottish Government's Code of Practice on Covert Surveillance & Property Interference, Dec 2017
[7] Police Act 1997
[8] Investigatory Powers Tribunal

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

12.3 Elected members on the Audit Risk and Scrutiny Committee receive reports on a quarterly basis regarding RIPSA activity and compliance. A review of the RIPSA protocol and procedure is also considered at the time the Annual report on RIPSA activity is presented to Committee.

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

13. Complaints

13.1 The Regulation of Investigatory Powers Act 2000 ("the UK Act") establishes an Independent Tribunal, called the Investigatory Powers Tribunal. This Tribunal has jurisdiction for authorisations granted under the Scottish Act.

13.2 The Tribunal is a court which investigates and determines complaints of unlawful use of covert techniques by public authorities which infringe on an individual's right to privacy.

14. Further Information

14.1 Further information about the Council's procedures for authorising Covert Surveillance can be accessed on the Khub and on the Intranet- http://thezone/cg/LegalServices/rm_covertsurveillance.asp

Also available on this page is:

- Scottish Government Covert Surveillance and Property Interference Code of Practice
- Scottish Government Covert Human Intelligence Sources Code of Practice
- Covert Surveillance and Property Interference- Revised Code of Practice, August 2018 https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/733218/201800802_CSPI_code_reformatted_for_publication__003_.pdf

14.2 Further advice on any aspect of Covert Surveillance procedures can be sought by any Service from Legal Services by contacting the Team Leader, Regulatory & Compliance on 2553 or 3168.

APPENDIX ONE

GUIDANCE NOTE ON PROPORTIONALITY

The term's ‘necessity’ and ‘proportionality’ are not defined within RIPSA, but are ‘imported from the European Convention on Human Rights.

'Necessity' is a concept which guards against the arbitrary interference with a citizen's rights. There are three statutory grounds of 'necessity' inherent in section 6(3) of RIPSA, namely;

- the prevention and detection of crime or prevention of disorder,
- the interests of public safety and
- the protection of public health.

In addition to this, the law requires the interference to be proportionate and in response to a pressing 'social need'.

'Proportionality' is a difficult concept to grasp but a paramount consideration for Officers who are responsible for completing and authorising Application forms for Directed Surveillance and the use of a Covert Human Intelligence Source or CHIS.

An illustration of how the Court assesses the 'proportionality test' can be found on the case of *Peck v UK*. Footage of Peck carrying a large knife was captured on CCTV cameras in Brentwood High Street, shortly after his attempt to commit suicide. The CCTV operator (an employee of Brentwood County Council) contacted the Police who arrested Peck and detained him under Mental Health legislation. A few months later, stills from the CCTV footage were used in an advertising campaign to promote the CCTV system.

Further to this, footage of Peck was broadcast on national television. Although Peck's face had been masked in one of the broadcasts, the masking was held to be inadequate, as persons who knew Peck could easily identify him from the footage. Peck then made an application to the European Court of Human

Rights on the grounds that his rights under Articles 8 (right to respect for private and family life) had been violated. Peck argued that it was the disclosure of that footage to the public in a manner in which he could never have foreseen which gave rise to such an interference.

In considering whether the interference with his right to privacy was proportionate, the Court had regard to:

1. the failure of the Council to attempt to identify Peck and seek his consent to the disclosure of the footage,

2. the failure of the Council to have 'masked' the image of Peck or enter into a written agreement with the media organisations ensuring that this would be done appropriately,

3. the strong interest the Government has in detecting and preventing crime by use of a CCTV system, and

4. the purpose for publishing the footage.

The Court held that Peck was a victim of a serious interference with his right to privacy involving national and local media coverage. In addition, disclosures by the Council of the CCTV material in *'CCTV news*' and to the '*Yellow Advertiser*', Anglia television, and the BBC were not accompanied by sufficient safeguards to prevent disclosure inconsistent with the guarantees of respect for the Peck's private life contained in Article 8. As such, the disclosure constituted a disproportionate and therefore unjustified interference with his private life and a violation of Article 8.

Officers should have in mind a wide range of factors when assessing whether an investigation is 'proportionate' to the achieved aim. Below is listed for information some considerations that should be taken into account. This list is not exclusive.

- <u>Interests affected</u>
  Identify whose and what interests are affected. Have you considered the risks involved and prepared for them?
- <u>Extent of interference</u>

Must have regard to the extent of the interference, have less intrusive measures been exhausted first , can you consult with other agencies?

- Duration of the interference
  Duration should not be excessive, consider planning, times and places of surveillance.

- Seriousness of the offence involved
  Is surveillance excessive in light of the offence involved? Is there a pressing social need?

- Availability of less intrusive alternatives of investigation
  Can the aim of the investigation be achieved without surveillance?

- Structured objectives
  Operational implications of the investigation

- Absence of irrationality, arbitrariness and unfairness
  Are you being unfair, have you made reasonable enquiries with the individual prior to considering surveillance, is what you wish to do relevant? Can you justify interfering with that person's human rights to achieve your aim?

- Relevant and sufficient reasons affected
  Be clear with your decision making and evidence on the application form that you have considered the above.

Ultimately, a balance will be required to be struck between the needs of society and the rights of individuals.

APPENDIX TWO

USING SOCIAL MEDIA AS AN INVESTIGATORY TOOL-THE DO'S AND DON'T'S

In a world where members of the public use social media as an ordinary communication tool, its unsurprising that public authorities recognise the opportunities to engage with members of the public and source information being held and posted on online sites such as Facebook, Twitter, Whatsapp, Instagram and others.

This note will provide guidance to officers who wish to use, or access online social sites to obtain or disclose information in pursuance of a regulatory function.

- **I am exercising a Council function and wish to search on social media sites to ascertain information to further my investigation.**

Staff should not use their personal social media account to undertake work related investigations.

If you undertake a search of an online social media site for the purposes of obtaining information about a person for a legitimate[1] regulatory function and you DO NOT have to take any "action" to do this covertly, it is unlikely that a Directed Surveillance authorisation would be required. This is because the individual has not set the privacy settings available and that data may be considered "open source". [i]

If you intend to access social media sites for a specific planned purpose on more than one occasion this may constitute Directed Surveillance and advice should be sought from the Regulatory & Compliance Team, Legal Services before engaging in planned repeated viewing.

If you are required to take further action within that site to obtain or gain access to information which is not viewable, you may require authorisation for Directed Surveillance. See below for further information.

- **I am exercising a Council function and want to create a profile on a social media site under a false name**.

It is not unlawful for a public authority like the Council to set up a false identity[2], but it is inadvisable for a member of a public authority to do so for a covert purpose without an authorisation for Directed Surveillance when private information is likely to be obtained. Officers wishing to use Social Media in this way should set out in the application for Directed Surveillance how this will be managed and what information they hope to obtain and for what use.

A member of a public authority should not adopt the identity of a person known, or likely to be known, to the subject of interest or users of the site without authorisation, and without the consent of the person whose identity is used and without the protection of that person. Their consent must be explicit.

- **I am exercising a Council function and want to start engaging with a specific person, or group of persons, on a social media site to obtain further information to assist my investigation.**

If you access social media sites using a false profile which you have created for the purposes of the investigation you will require a Directed Surveillance authorisation. If you then wish to start communicating with that person for the purposes of establishing a relationship for a covert purpose, you will require an authorisation for a Covert Human Intelligence Source.

- **I wish to create a group profile which is overt (promotes a service of Aberdeen City Council) for the purposes of a regulatory function.**

There is no legal requirement[3] for any authorisation for this activity. Any person engaging with the Group Profile will be aware that it is an Aberdeen City Council Service. However, you will have to consider the implications of consent and privacy prior to engaging with members of the public in this way. Consideration should be had to the type of service being promoted, the age of the person with whom you are engaging, the security and information management requirements around this type of engagement and the right of the person to respect their private life and correspondence.

APPENDIX THREE-

IDENTIFYING WHEN A HUMAN SOURCE BECOMES A CHIS

The definition of a Covert Human Intelligence Source (CHIS) is a person who establishes or maintains a personal or other relationship with a person(s) to obtain or access information covertly, or to provide access to information or disclose information obtained by the covert relationship. Even though a person is not considered a CHIS, the Council may still have a duty of care towards the safety and welfare of a person who provides a member of staff with information/ intelligence.

In previous inspections, the Commissioner highlighted that there may be officers within the Council whom are receiving information from, or asking a member of the public to provide them with information, about a specific person or persons for a legitimate purpose, without that person or persons knowledge. In these circumstances, ACC staff need to be clear what implications there are for these types of arrangements and whether any authorisations for covert surveillance would be required.

Ultimately, if information is being provided to the Council by a member of the public and that information is being recorded as potentially useful or actionable, there is a duty of care to the individual providing that information and the onus is on the Council to manage that that arrangement properly.
Staff should consider the personal circumstances of the person; are they vulnerable, reliable, is there an existing relationship to the target (person staff are interested in), are they volunteering the information or exploiting a relationship they have as they are already known to the individual, are they clear about the implications of providing the information, are they putting themselves at risk by providing the information or continuing to provide it? Where staff request someone exploit an existing relationship for a covert purpose, they should ensure that that person is protected and safe during the period of the arrangement. Further, staff should also consider the risks to a volunteer who continues to provide information about a person or persons; are they putting themselves at risk by doing so having regard to the circumstances? Staff should also ensure that the person providing the information or being tasked to provide it, understands the impact of doing that; will they need to make a statement in later proceedings and/ or can they remain anonymous?

Set out below is the guidance from the Scottish Government and the Office of the Surveillance Commissioner on this area.

Human source activity falling outside CHIS definition

Not all human source (person providing information) activity will meet the definition of a CHIS. For example, a source may be a member of the public who volunteers information he/she has witnessed or knows about.

Public

In many cases involving sources, a relationship will not have been established or maintained for a covert purpose. Many sources merely volunteer or provide information that is within their personal knowledge, without being induced, asked, or tasked by a public authority. This means that the source is not a CHIS for the purposes of RIP(S)A and no authorisation under RIP(S)A is required.

Example 1: A member of the public volunteers a piece of information to a member of a public authority regarding something he has witnessed in his neighbourhood. The member of the public would not be regarded as a CHIS. He is not passing information as a result of a relationship which has been established or maintained for a covert purpose.

This would be the case for any intelligence gathered by officers of the Council where this has been volunteered. If the member of the public knows certain information which he/she volunteers due to an existing relationship and is asked to maintain that relationship and feedback information on an aspect of that relationship, then a CHIS may be appropriate.

Professional or statutory duty

Certain individuals will be required to provide information to public authorities or designated bodies out of professional or statutory duty. Any such regulatory or professional disclosures should not result in these individuals meeting the definition of a CHIS, as the business or professional relationships from which the information derives will not have been established or maintained for the covert purpose of disclosing such information.

Furthermore, this reporting is undertaken “in accordance with the law” and therefore any interference with an individual’s Article 8 rights will satisfy that requirement of Article 8(2).

This statutory or professional duty, however, would not extend to the situation where a person is asked to provide information which they acquire as a result of an existing professional or business relationship with the subject but that person is under no obligation to pass it on.

Tasking not involving relationships

Tasking a person to obtain information covertly may result in authorisation under RIP(S)A being appropriate. However, this will not be true in all circumstances. For example, where the tasking given to a person does not require that person to establish or maintain a relationship for the purpose of obtaining, providing access to or disclosing the information sought or where the information is already within the personal knowledge of the individual, that person will not be a CHIS.

Example: A member of the public is asked by a member of a public authority to maintain a record of all vehicles arriving and leaving a specific location or to record the details of visitors to a neighbouring house. A relationship has not been established or maintained in order to gather the information and a CHIS authorisation is therefore not available. Other authorisations under RIP(S)A eg for directed surveillance may need to be considered where there is an interference with the Article 8 rights of an individual.

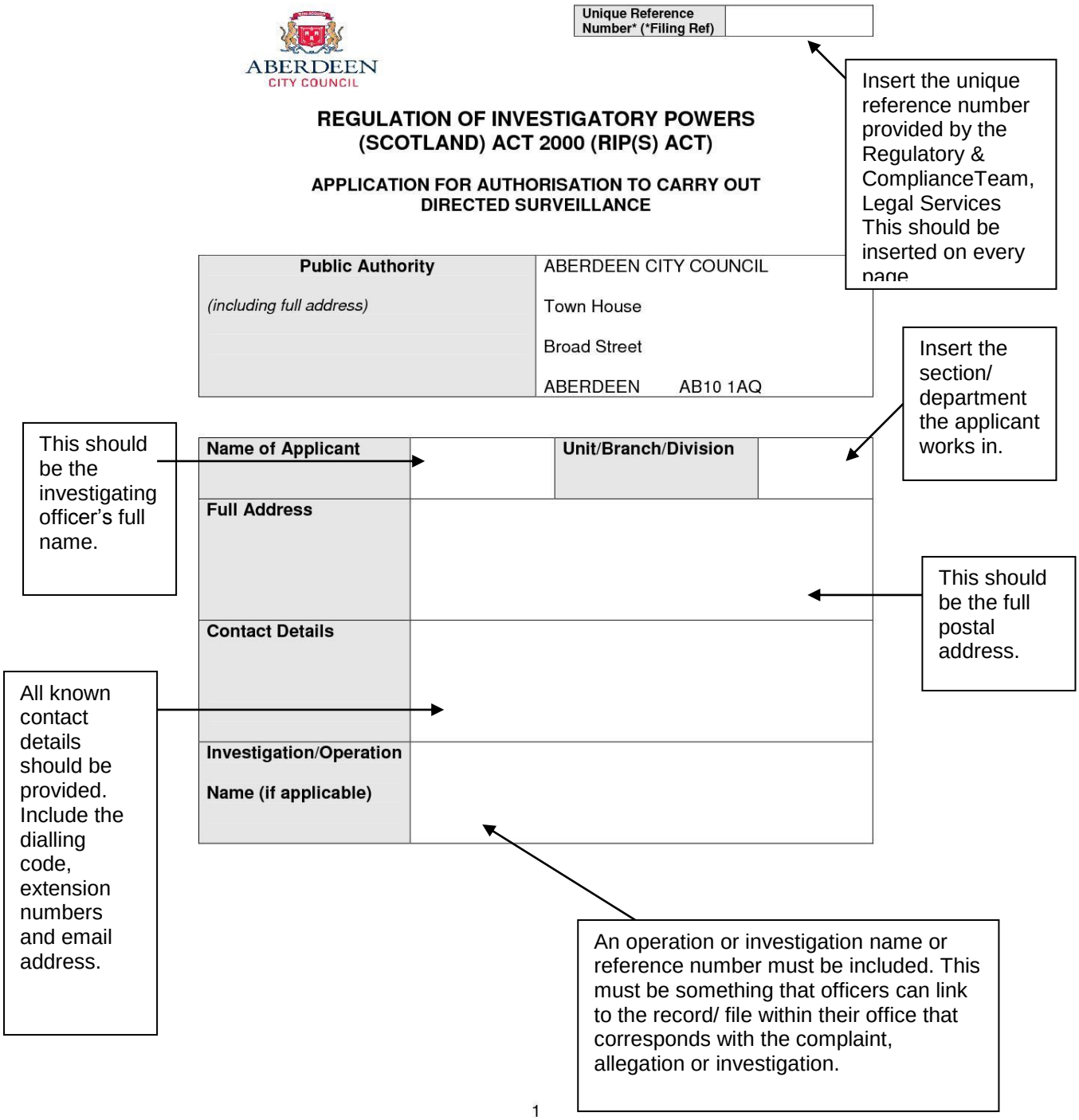
Identifying when a human source becomes a CHIS

Determining the status of an individual or organisation is a matter of judgement by the public authority. Public authorities should avoid inducing individuals to engage in the conduct of a CHIS either expressly or implicitly without obtaining a CHIS authorisation.

However, the tasking of a person should not be used as the sole benchmark in seeking a CHIS authorisation. It is the activity of the CHIS in exploiting a relationship for a covert purpose which is ultimately authorised by RIP(S)A, whether or not that CHIS is asked to do so by a public authority. It is possible therefore that a person will become engaged in the conduct of a CHIS without a public authority inducing, asking or assisting the person to engage in that conduct.

APPENDIX FOUR

GUIDE TO COMPLETING PART 1- APPLICATION FORM[9]



ABERDEEN CITY COUNCIL

Unique Reference Number* (*Filing Ref)	

Insert the unique reference number provided by the Regulatory & ComplianceTeam, Legal Services This should be inserted on every page

REGULATION OF INVESTIGATORY POWERS (SCOTLAND) ACT 2000 (RIP(S) ACT)

APPLICATION FOR AUTHORISATION TO CARRY OUT DIRECTED SURVEILLANCE

Public Authority *(including full address)*	ABERDEEN CITY COUNCIL Town House Broad Street ABERDEEN AB10 1AQ

Insert the section/ department the applicant works in.

This should be the investigating officer's full name.

Name of Applicant		**Unit/Branch/Division**	
Full Address			
Contact Details			
Investigation/Operation Name (if applicable)			

This should be the full postal address.

All known contact details should be provided. Include the dialling code, extension numbers and email address.

An operation or investigation name or reference number must be included. This must be something that officers can link to the record/ file within their office that corresponds with the complaint, allegation or investigation.

1

[9] Whilst the format of the form has been amended, the content is still the same. The Authorising Officer's part is now contained in a separate form; Part 2- Authorisation Form.

Unique Reference Number* (*Filing Ref)	

Details of application:

1. Give rank or position of authorising officer in accordance with The Regulation of Investigatory Powers (Prescription of Offices, Ranks and Positions) (Scotland) Order 2000, No 343; The Regulation of Investigatory Powers (Prescription of Offices, Ranks and Positions) (Scotland) Amendment Order 2001, No. 87; and The Regulation of Investigatory Powers (Prescription of Offices, Ranks and Positions) (Scotland) Amendment (No. 2) Order 2003, No. 50 [1]

It is a statutory requirement that certain officers are granted powers to authorise surveillance. In ACC this is the Director, Head of Service or Third Tier officer, where appropriate.
The full job details of the authorised officer must be inserted here including their level in ACC. For up to date information, see the Intranet or Khub.

Why are you investigating this subject matter, what piece of legislation empowers you to undertake an investigation and enforce that particular law/ offence? What delegated powers to you have?

2. Describe the conduct to be authorised and purpose of the investigation or operation.

3. Identify which grounds the directed surveillance is <u>necessary</u> under section 6(3) of RIP(S) Act. *delete as inapplicable*
• For the purpose of preventing or detecting crime or of preventing disorder; • In the interests of public safety; • For the purpose of protecting public health.

One of the grounds must be selected and the other non relevant grounds deleted. If you select the first ground, you will be required to detail what alleged crime/ offence has been committed. If you cannot satisfy a ground you should not continue with the application.

1 For Local authorities: The exact position of the authorising officer should be given. For example, Head of T
rather than officer responsible for the management of an investigation.

Unique Reference Number* (*Filing Ref)	

4. Explain why directed surveillance is necessary in this particular case.

You are required to explain why a covert operation will obtain the information you want

5. Explain why the directed surveillance is proportionate to what it seeks to achieve (*why is the intrusion outweighed by the need for surveillance in operational terms or can the evidence be obtained by any other means?)*

Expanding on what you've put in 4. above, be clear about what efforts you've made to ascertain the information prior to this application e.g. house visits, written communication. Is what you are intending on doing excessive, is there a less intrusive way to get the information/ intelligence required? Have previous attempts of ascertaining the information failed?

e nature of the surveillance to be authorised, including any premises or hicles involved (e.g. camera, binoculars, video recorder) that may be ed.

You should include in this section whether surveillance is static, on foot, in a vehicle or a residence. Also what the surveillance involves; cameras, video, photographs, visual monitoring equipment, notebooks etc, whether a corroborating officer will be undertaking the surveillance; the times and location of the surveillance e.g the postal address. If you have a map of the area you are carrying out the surveillance in, mark this up and attach this to the application form.

vestigation or operation to be carried out. The identities, where known, those to be subject of the directed surveillance.

ame:
ddress:
O. B:

her information as appropriate:

Where this information is known please ensure you insert it. If you have a description of the subject of surveillance then this should also be included. If you do not know the details of the subject, clarify why these details aren't known.

Unique Reference Number* (*Filing Ref)	

8. Explanation of the information which it is desired to obtain as a result of the directed surveillance.

You should include here what you want the surveillance to provide. This can be an expansion or repetition of 2.

9. Details of risk assessment on the security and welfare of those carrying out the directed surveillance.

Either include a copy of a risk assessment or detail what the risks are, how you have planned to minimise them and what exit strategy you have employed. Always have regard to the type of location someone is being tasked to observe/ visit.

10. Collateral intrusion.

THE USE OF DIRECT SURVEILLANCE WITHIN THE PUBLIC DOMAIN WILL LEAD TO COLLATERAL INTRUSION OF OTHERS NOT ENGAGED IN SUSPECTED ILLEGAL OR CRIMINAL ACTIVITY. PERSONS WHO HAVE LEGITIMATE ACCESS TO AREAS WHICH ARE SUBJECT TO COVERT SURVEILLANCE MAY BE SUBJECTED TO COLLATERAL INTRUSION. ALL REASONABLE EFFORTS MUST BE MADE TO MINIMISE COLLATERAL INTRUSION. THIS WILL INCLUDE:

- UTILISATION OF TRAINED SURVEILLANCE OPERATIVES WITH APPROPRIATE KNOWLEDGE AND EXPERTISE
- FOCUSING OF SURVEILLANCE ON THE SUBJECTS OF AUTHORISATION
- DAILY BRIEFING AND DEBRIEFING OF AND TO LINE MANAGERS
- CONSTANT REVIEW AND ASSESSMENT OF OPERATIONAL TACTICS.

INDICATE THE EXTENT OF ANY POTENTIAL FOR COLLATERAL INTRUSION ON PERSONS OTHER THAN THOSE TARGETED: (INCLUDING DETAILS IN THE BOX BELOW OF PLANS TO MINIMISE COLLATERAL INTRUSION)

In this section you need to be clear as to the potential for collateral intrusion. If others may also be surveyed, you need to identify how you will minimise this risk, if possible and what steps you'll take to record your observations.

Unique Reference Number* (*Filing Ref)	

11. Confidential Information

INDICATE THE LIKELIHOOD OF ACQUIRING ANY CONFIDENTIAL INFORMATION:

12. Anticipated Start	Date:	Time:

13. Applicant's Details

Name (print) **Tel No:**

Grade/Rank **Date:**

Signature

14. Confirmation of urgent authorisation: details of why application is urgent.

15. Authorising Officer's comments explaining why in his view the directed surveillance is necessary and proportionate. <u>This box must be completed</u>.

Confidential information is information which is subject to legal professional privilege (communications between a professional legal adviser and their client), personal information (such as information relating to someone's physical or mental health e.g. medical records) and journalistic material, e.g. the source of information. Any investigation/ operation which is likely to obtain confidential information should be authorised by the Chief Executive.

This section is to be completed by the Applicant

In this section the Authorising Officer needs to expand on why the surveillance is required, and why having regard to all the circumstances, it should be authorised.

An urgent authorisation may be authorised if an officer was out on official duty but not working under an authorisation and the authorising officer was of the view that the time taken to authorise the surveillance would be likely to endanger life or jeopardise the investigation or operation for which the authorisation was being sought. Details of the time, date and reason for granting an urgent authorisation should be completed by the Authorising Officer who sanctioned it.

Unique Reference Number* (*Filing Ref)	

16. Authorising Officer's Statement			
I, [insert name], hereby authorise the following directed surveillance investigation/operation [ ]. This authorisation will cease to have effect at the end of the period of three months commencing on the date of authorisation, unless renewed in writing (see separate form for renewals). This authorisation will be reviewed frequently (see below) to assess the need for the authorisation to continue.			
Name (Print):		**Grade/Rank:**	
Signature:		**Date:**	
		Time:	

Date of first review:	
Date of subsequent reviews of this authorisation:	

In this section the Authorising Officer should explain in his/her own words What is being authorised, Why the surveillance is necessary, whom the surveillance will be directed against, Where and When it will take place, what surveillance activity/ equipment will be used and How is it to be achieved.

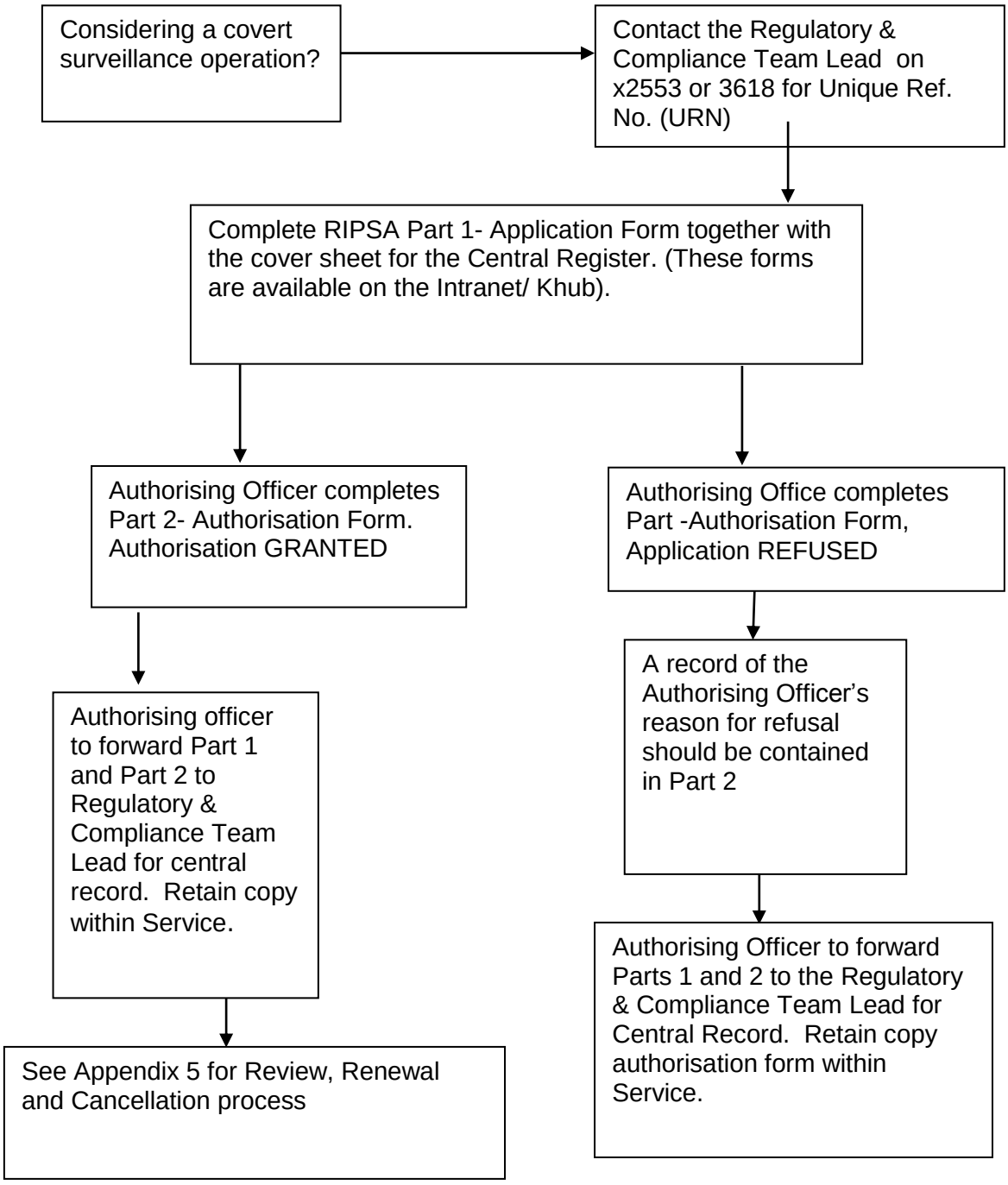
16. Confidential Information Authorisation.

Name (Print)		**Grade/Rank**	
Signature		**Date**	

This section should be completed by the Chief Executive and should set out why it's necessary and proportionate to obtain confidential information having regard to the particular investigation.

APPENDIX FIVE-

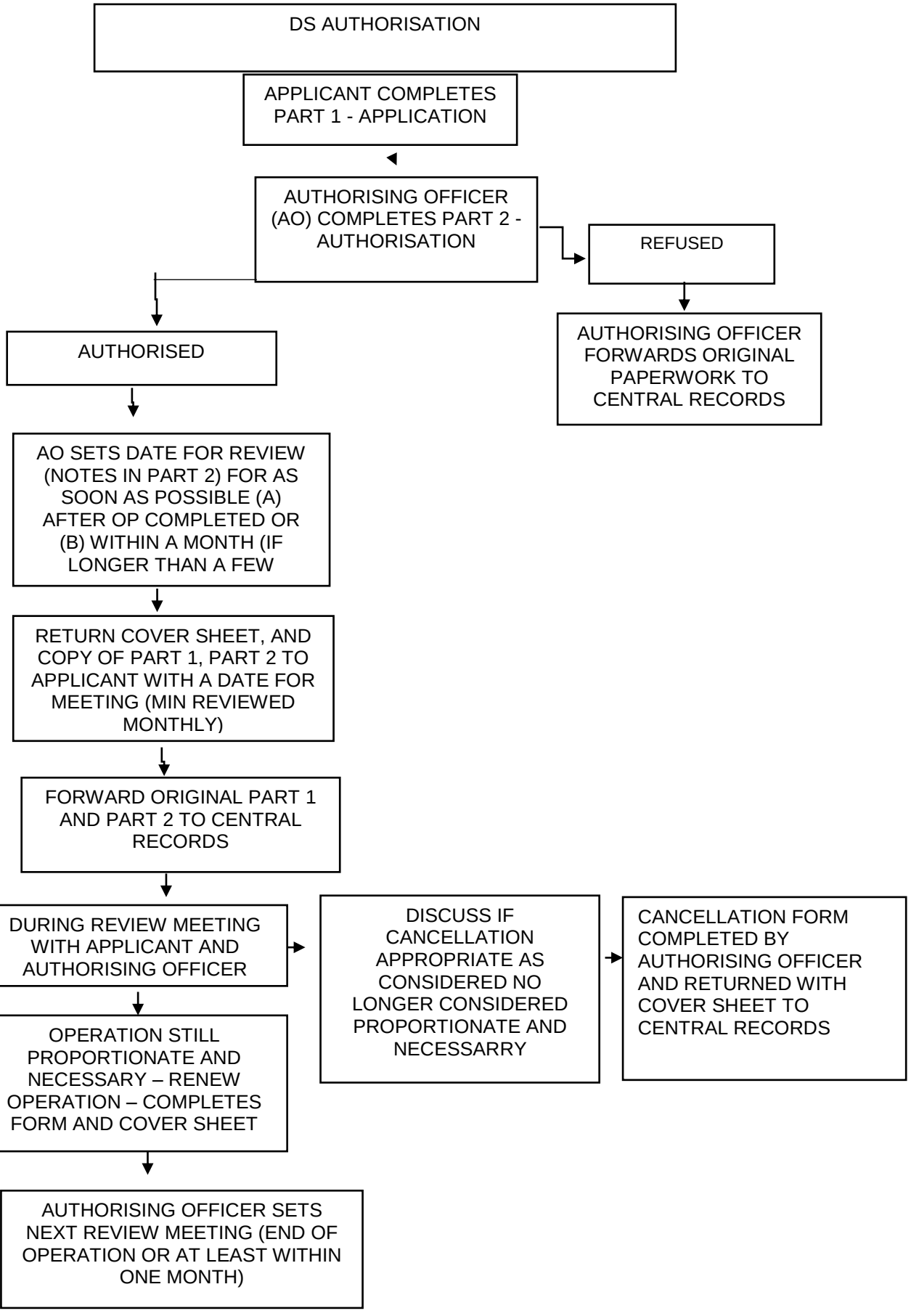
RIPSA AUTHORISATION PROCESS



REMEMBER - it's the AUTHORISING OFFICER'S responsibility to ensure that the surveillance operation is cancelled, renewed and reviewed timeously.

APPENDIX SIX-

REVIEW, RENEWAL AND CANCELLATION PROCESS



APPENDIX SEVEN –

RIPSA TRAINING POLICY

Introduction

This policy outlines the training that will be provided across Aberdeen City Council in connection with powers under RIPSA to conduct Covert Surveillance in certain, limited circumstances.

The aim of this policy is to ensure that, across the organisation a high level of awareness of the restraints of undertaken covert surveillance exists and, where necessary, training of a suitably detailed nature is delivered in order that Officers are familiar with the legal and procedural requirements relating to Covert Surveillance. A further aim of the Training Policy is to ensure that those Officers who undertake Directed Surveillance and Covert Human Intelligence Source (CHIS) applications and those Officers appointed as Authorising Officers for such applications receive regular opportunities to refresh and update their knowledge and skills in this area.

Classification of Job Roles

For the purposes of identifying RIPSA training requirements, all job roles within Aberdeen City Council will be classified into one of four tiers.

Tier	Description	Example Job Roles
Tier 0	RIPSA Authorising Officers (including the Chief Executive and Directors who, in the absence of the Chief Executive deputise as the Head of Paid Service) Officers within Legal Services with responsibility for oversight of RIPSA.	 Solicitors Legal Team Leaders
Tier 1	Job Roles held by Officers who do or will prepare applications for consideration by a RIPSA Authorising Officer.	Trading Standards Officers Environmental Health Officers Fraud Officers Service Manager – Community Safety
Tier 2	Job Roles identified as those which have an Investigative or Enforcement function.	Anti-Social Behaviour Investigation Officers City Wardens Social Workers Licensing Standards Officers Human Resources Advisers / Investigatory Officers
Tier 3	All other job roles.	

Training Requirements

Tier 0 Roles: Officers identified in Tier 0 roles must attend RIPSA Authorising Training as soon as possible following their appointment. No Officer in Tier 0 will be permitted to Authorise or Review an Application for Covert Surveillance prior to having attended this training.

Officers should receive refresher training every 2 – 3 years and receive Update Bulletins, including practice improvement notes developed from previous applications, on at least one occasion per year.

Tier 1 Roles: Officers identified in Tier 1 roles must attend RIPSA in Practice Training as soon as possible following their appointment. No Officer in Tier 1 will be permitted to make a Directed Surveillance or CHIS Application prior to having attending this training.

Officers in Tier 1 should attend refresher training every 2 -3 years and will receive Information Bulletin updates as appropriate.

Tier 2 Roles: Officers will be reminded, via a rolling campaign of Information Posters and banners, of the importance of considering whether covert surveillance of individuals is being undertaken and of appropriate steps being taken to regulate such activity prior to it being undertaken.

If any Officer identified as being in Tier 2 requires to make an application for authorising of Directed Surveillance or CHIS, they will require to complete the RIPSA in Practice Training detailed in Tier 1 above prior to doing so.

Tier 3 Roles: Officers in Tier 3 will be exposed to the rolling campaign of Information Posters and Intranet banners which will seek to raise awareness of Covert Surveillance and the need for such activity to be properly authorised prior to taking place.

Any Officer in Tier 3 who recognises that they may partake in Covert Surveillance as part of their job role will be required to complete the RIPSA in Practice Training outlined in Tier 1 above as soon as possible following this recognition.

Review

This training policy will be kept under review by Officers in Legal Services and will be subject to a formal review not more than three years following implementation.

Appendix One