Bridgend County Borough Council

Policy on Directed Surveillance and Covert Human Intelligence Sources under the Regulation of Investigatory Powers Act 2000

Contents

1 Introduction to RIPA 2000

2 Types of Surveillance

3 Authorisation of Surveillance
Necessity and Proportionality
Duration
Renewals
Cancellations
Reviews

4 Drive-bys

5 CCTV

6 Internet and Social Networking Sites

7 Covert Human Intelligence Source (CHIS)

8 Collaborative Working

9 Record Management

10 General Considerations

Appendices

1 Identification of Senior Responsible Officer and Designated Authorised Officers

2 RIPA Authorisation Flow Chart

3 Home Office Local Authority Procedure Flow Chart: Application to a Justice of the Peace seeking an Order to approve the grant of a RIPA Authorisation or Notice.

Introduction to RIPA 2000

1.1 In carrying out its duties the Council may need to conduct appropriate investigations into allegations or concerns brought to its attention and such investigations may necessarily require covert surveillance. The Regulation of Investigatory Powers Act 2000 (RIPA) provides a regulatory framework governing interception of communications, surveillance and associated activities. This is to ensure the powers are used lawfully and in a way that is compatible with Human Rights. Through the application of authorisation procedures and Magistrates Court approval it ensures that a balance is maintained between the public interest and the human rights of individuals.

1.2 This Policy is based upon the requirements of RIPA and Home Office's Code of Practices on Covert Surveillance and Covert Human Intelligence Sources. Copies of the Home Office's Codes of Practice are available on their website. Forms to record applications and decisions in writing are also available on the website.

1.3 The Council takes its statutory responsibilities seriously and will at all times ensure that any such surveillance or use of an intelligence source carried out is authorised and in accordance with the legislation. Investigations which are not authorised could leave the Council open to challenge by individuals who consider that there has been an intrusion into their privacy.

1.4 It is considered good practice for public authorities to appoint a Senior Responsible Officer (SRO) to be made responsible for the integrity of the process in place for the management of surveillance. The current SRO for the Council is identified in **Appendix 1**. Whilst legislation does not preclude the SRO's use as an Authorising Officer, it is unlikely that they would be regarded as objective if they oversee their own authorisations.

Types of Surveillance

2.1 Surveillance can be overt or covert. Overt surveillance does not require authorisation under RIPA and covers all situations where surveillance is not covert. The use of such surveillance is to be commended where the required result can be achieved by this means.

2.2 Covert surveillance is carried out in a manner calculated to ensure that the person subject to the surveillance is unaware that it is or may be taking place.

2.3 There are three types of covert surveillance:

'Intrusive Surveillance' - t**he Council has no statutory power to grant authorisations for intrusive surveillance but it is included here to alert officers to be aware of inadvertently breaching this rule.**

Intrusive surveillance is covert and carried out in relation to anything taking place on any residential premises or any private vehicle. Anything that occurs on residential premises or any private vehicle and involves the presence of someone on the

premises or in the vehicle or is carried out by means of a surveillance device will be intrusive. If the device is not on the premises or in the vehicle, it is only intrusive if it consistently produces information of the same quality as if it were.

Residential Premises includes any premises as is for the time being occupied or used by any person, however, temporary, for residential purposes or otherwise as living accommodation. It will not include communal areas, front gardens or driveways visible to the public.

Private vehicles will be those used primarily for the private purpose of the person who owns it or a person otherwise having the right to use it.

'Directed Surveillance' – this is covert surveillance that is not intrusive and is undertaken for the purposes of a specific investigation in a way that is likely to produce private information about a person. It must be necessary and proportionate to what it seeks to achieve.

'Covert Human Intelligence Source' (CHIS) – this is the use or conduct of someone who establishes or maintains a personal or other relationship with a person for the covert purpose of obtaining information. It must be necessary and proportionate to what it seeks to achieve.

Authorisation for Surveillance

3.1 As soon as a plan of action is decided upon which involves covert surveillance or the use of CHIS appropriate authorisation should be sought in advance.

3.2 All RIPA authorisations will require Magistrates Court approval in the form of an Order to take effect. The Home Office guidance on the judicial approval process for RIPA is available on the Home Office website.

3.3 The procedure outlined in the flowchart at **Appendix 2** should be followed by Officers to ensure formal quality assurance.

3.4 All applications for authorisation of directed surveillance must be in writing and stipulate:

- how the surveillance will be conducted;
- the grounds on which authorisation is sought. Authorisations cannot be granted unless specific criteria are satisfied. **For the Council, the only ground for authorisation is for the purpose of preventing or detecting crime which -**
  (a) constitutes one or more criminal offences, or
  (b) is, or corresponds to, any conduct which, if it all took place in England and Wales, would constitute one or more criminal offences.

  And the criminal offence or one of the criminal offences is or would be-

  (a) an offence which is punishable, whether on summary conviction or on indictment, by a maximum term of at least 6 months of imprisonment, or
  (b) an offence under:
  - section 146 of the Licensing Act 2003 (sale of alcohol to children);
  - section 147 of the Licensing Act 2003 (allowing the sale of alcohol to children);

- section 147A of the Licensing Act 2003 (persistently selling alcohol to children);
- section 7 of the Children and Young Persons Act 1933 (sale of tobacco, etc, to persons under eighteen)

- a full account of the investigation or operation (including full details of where the surveillance is to take place);
- likelihood of acquiring any confidential material as a consequence of the surveillance;
- the details of any potential collateral intrusion and an assessment of the risk of such intrusion or interference. There is an obligation on officers to ensure that collateral intrusion is minimised and is not excessive in the circumstances
- the reasons why the directed surveillance is considered to be proportionate to what it seeks to achieve (including the relevant circumstances);
- the identities, where known, of those to be the subject of directed surveillance;
- an explanation of the information which it is desired to obtain as a result of the authorisation;
- where the authorisation is sought urgently, reasons why the case is considered to be urgent;
- a subsequent record of whether authority was granted or refused, by whom and the time and date.

3.5 Applications to the Court for an approval of an authorisation must be made in accordance with the requirements of the Court. Legal Services must be consulted on the application form to the Magistrates Court.

The applicant must:

- apply in writing and serve the application on the court officer;
- attach the authorisation or notice which the applicant wants the court to approve;
- attach such other material (if any) on which the applicant relies to satisfy the court of the statutory requirements;
- attach the proposed terms of the Order (Annex B court document);
- the forms and supporting documentation MUST make the case it is not enough for an officer to provide oral evidence not supported by the contents of the paper;
- provide the court (on request) with a signed Delegated Power authorising the appearance of the local authority in legal proceedings.

3.6 **Appendix 3** outlines the local authority procedure for seeking an order from the Magistrates Court.

3.7 The Officers within the Council entitled to grant authorisations are specified in legislation and are those whose posts appear in **Appendix 1**, however it is important that all those involved in undertaking surveillance are fully aware of the extent and limits of the authorisation in question.

3.8 Wherever knowledge of confidential information is likely to be acquired, a higher level of authorisation is needed. Confidential information consists of communications subject to legal privilege, communications between a Member of

Parliament and another person on constituency matters, confidential personal information, or confidential journalistic material. So, for example, extra care should be taken where, through the use of surveillance, if it is likely that knowledge will be acquired of communications between a minister of religion and an individual relating to the latter's spiritual welfare, or between a Member of Parliament and a constituent relating to constituency matters, or wherever matters of medical or journalistic confidentiality or legal privilege may be involved. Authorisation can only be provided by the Chief Executive or in his/her absence the Monitoring Officer.

3.9 Authorising Officers should not be responsible for authorising their own activities. Because of the number of officers designated as Authorising Officers within the Council, this situation should be avoidable.

Necessity and Proportionality

3.10 In signing the application an Authorising Officer must give personal consideration to the necessity and proportionality of the proposed surveillance prior to applying to the Magistrates for approval and must personally ensure that the surveillance is reviewed and cancelled.

3.11 Proportionality will involve balancing the seriousness of intrusion into the privacy of the subject of the operation (or any other person who may be affected) against the need for the activity in investigative and operational terms. The authorisation will not be proportionate if it is excessive in the overall circumstances of the case. Each action authorised should bring an expected benefit to the investigation or operation and should not be disproportionate or arbitrary. The fact that a suspected offence may be serious will not alone render intrusive actions proportionate. Similarly, an offence may be so minor that any deployment of covert techniques would be disproportionate.

3.12 No activity should be considered proportionate if the information which is sought could reasonably be obtained by other less intrusive means. The following elements of proportionality should be considered:

- balancing the size and scope of the proposed activity against the gravity and extent of the perceived crime or offence;
- explaining how and why the methods to be adopted will cause the least possible intrusion on the subjects and others;
- considering whether the activity is an appropriate use of the legislation and a reasonable way, having considered all reasonable alternatives, of obtaining the necessary result;
- evidencing, as far as practicable, what other methods had been considered and why they were not implemented.

3.13 If the Authorising Officer is unsure on any matter they should seek advice from the SRO.

3.14 Urgent authorisations should not be necessary. An authorisation is not to be regarded as urgent where the need for an authorisation has been neglected or the urgency is of the Authorising Officer's or Applicant's own making. The Magistrates Court may consider an authorisation out of hours in **exceptional** circumstances. Please refer to **Appendix 3** for the procedure to be followed when an authorisation is urgent and cannot be handled the next working day.

3.15 Officers conducting covert surveillance will have a full briefing and be required to read the authorisation granted to ensure that their activity is based on what has been specifically authorised and not merely what has been requested.

Duration

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

3.17 As soon as the decision is taken that directed surveillance should be discontinued, the instruction must be given to those involved to stop all surveillance. The date and time when such an instruction was given should be recorded.

Renewals

3.18 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, he may renew it in writing for a further period of three months. Applications for renewal should only be made shortly before the authorisation is due to expire and must be submitted to the Magistrates Court for approval before they can be effective.

3.19 Authorisations may be renewed more than once if necessary, provided they continue to meet the criteria for authorisation and are approved by the Magistrates Court.

3.20 All applications for the renewal of an authorisation should record:

- whether this is the first renewal or every occasion on which the authorisation has been renewed previously;
- any significant changes to the information as outlined in the original application;
- the reasons why it is necessary to continue with the surveillance;
- the content and value to the investigation or operation of the information so far obtained by the surveillance;
- the results of regular reviews of the investigation or operation.

3.21 In rare circumstances renewals may be granted orally in urgent cases but will still require the approval of the Magistrates Court.

Cancellations

3.22 The Authorising Officer who granted or last renewed the authorisation must cancel it if s/he is satisfied that the directed surveillance no longer meets the criteria upon which it was authorised. The cancellation should include how the surveillance assisted the investigation. When cancelling an authorisation, an Authorising Officer must ensure that proper arrangements have been made for the activity's discontinuance, including the removal of any technical equipment. Where the Authorising Officer is no longer available, this duty will fall on any one of the other Authorising Officers listed at **Appendix 1**.

Reviews

3.23 Reviews of authorisations should be undertaken on a monthly basis to assess the need for the surveillance to continue. The results of a review should be recorded.

Where the surveillance provides access to confidential information or involves collateral intrusion authorisations for such surveillance should be reviewed frequently.

3.24 If the Authorising Officer is in any doubt they should ask the SRO before any directed surveillance is authorised, renewed, cancelled or rejected.

Drive-bys

4.1 'Drive-by' surveillance may or may not need a RIPA authorisation and it is not acceptable to prescribe a minimum number of passes before an authorisation is required. Where an officer as part of an investigation, intends to drive by a property to establish the location of a property then an authorisation is unlikely to be required. However, if the drive-by is to assess for signs of occupation and a record is to be made or the drive-bys are repeated and/or systematic, then an authorisation may be required. Consideration should also be given to the likelihood of collateral intrusion.

CCTV

5.1 The use of overt CCTV cameras does not normally require an authorisation as members of the public will be aware that such systems are in use (e.g. visible signage). However, where overt CCTV cameras are used in a covert and pre-planned manner as part of a specific investigation or operation, an authorisation should be considered.

5.2 If a law enforcement agency (eg Police) wishes to use the Council's CCTV system for directed surveillance, a copy of the authorisation will be required (redacted if necessary to prevent the disclosure of sensitive information) and the equipment will only be used in accordance with the authorisation.

Internet and Social Networking Sites

6.1 Although social networking and internet sites are easily accessible, consideration must still be given about whether a RIPA authorisation should be obtained if they are going to be used during the course of an investigation. If the study of an individual's online presence becomes persistent, or where material obtained from any check is to be extracted and recorded and may engage privacy considerations, RIPA authorisations may need to be considered.

6.2 Care must be taken to understand how the social media site being used works. Officers must not be tempted to assume that one service provider is the same as another or that the services provided by a single provider are the same.

6.3 Depending on the nature of the online platform, there may be a reduced expectation of privacy where information relating to a person or group of people is made openly available within the public domain, however in some circumstances privacy implications still apply. This is because the intention when making such information available was not for it to be used for a covert purpose such as investigative activity. This is regardless of whether a user of a website or social media platform has sought to protect such information by restricting its access by activating privacy settings.

6.4 In order to determine whether a directed surveillance authorisation should be sought for accessing information on a website as part of a covert investigation or

operation, it is necessary to look at the intended purpose and scope of the online activity it is proposed to undertake. Factors that should be considered in establishing whether a directed surveillance authorisation is required include:

- Whether the investigation or research is directed towards an individual;
- Whether it is likely to result in obtaining private information about a person or group of people;
- Whether it is likely to involve visiting internet sites to build up a picture or profile;
- Whether the information obtained will be recorded and retained;
- Whether the information is likely to provide an observer with a pattern of lifestyle;
- Whether the information is being combined with other sources of information, which amounts to information relating to a person's private life;
- Whether the investigation or research is part of an ongoing piece of work involving repeated viewing of the subject(s);
- Whether it is likely to involve identifying and recording information about third parties, such as friends and family members of the subject of interest, or information posted by third parties, that may include private information and therefore constitute collateral intrusion into the privacy of these third parties.
- Conversely, where the Council has taken reasonable steps to inform the public or particular individuals that the surveillance is or may be taking place, the activity may be regarded as overt and a directed surveillance authorisation will not normally be available.

Example 1: *An officer undertakes a simple internet search on a name, address or telephone number to find out whether a subject of interest has an online presence. This is unlikely to need an authorisation. However, if having found an individual's social media profile or identity, it is decided to monitor it or extract information from it for retention in a record because it is relevant to an investigation or operation, authorisation should then be considered.*

Example 2: *The Council undertakes general monitoring of the internet in circumstances where it is not part of a specific, ongoing investigation or operation to identify themes, trends, possible indicators of criminality or other factors that may influence operational strategies or deployments. This activity does not require RIPA authorisation. However, when this activity leads to the discovery of previously unknown subjects of interest, once it is decided to monitor those individuals as part of an ongoing operation or investigation, authorisation should be considered.*

6.5 An authorisation for the use and conduct of a CHIS (see paragraph 7) may be needed if a relationship is established or maintained by the officer on behalf of the Council without disclosing his or her identity (i.e the activity will be more than mere reading of the site's content). This could occur if an officer covertly asks to become a 'friend' of someone on a social networking site.

6.6 It is not unlawful for an officer to set up a false identity but it is inadvisable to do so for a covert purpose without authorisation.

6.7 An officer should not adopt the identity of a person known, or likely to be known, to the subject of interests or users of the site without authorisation, and without the explicit consent of the person whose identity is used, and without considering the protection of that person.

Covert Human Intelligence Source (CHIS)

7.1 Under the 2000 Act, a person is a CHIS if:

- they establish or maintain a personal or other relationship with a person for the covert purpose of facilitating the doing of anything falling within paragraph 26(8)(b) or (c) of the Act;
- they covertly use such a relationship to obtain information or to provide access to any information to another person; or
- they covertly disclose information obtained by the use of such a relationship or as a consequence of the existence of such a relationship.

7.2 **Urgent advice from Legal should be sought should the use and conduct of a CHIS be considered. The Council is not required to seek or obtain an authorisation just because one is available. The use or conduct of a CHIS can be a particularly intrusive and high risk covert technique, requiring dedicated and sufficient resources, oversight and management**.

7.3 There is a separate Code of Practice for CHIS issued by the Home Office which officers should carefully study if a CHIS authorisation is sought. The same principles outlined above for directed surveillance apply to CHIS and should be followed including necessity and proportionality.

7.4 Officers should consider the security and welfare of the source and the foreseeable consequences to others in relation to what they are being asked to do. A risk assessment must be carried out before any authorisation is granted, at any renewal, review and cancellation.

7.5 Following authorisation and approval from the Magistrates Court, one officer is to be tasked with the day to day running of the CHIS, contact with them, giving them their tasks and keeping confidential records about what they achieve. A separate officer is to be appointed to oversee the use made of the CHIS.

7.6 An authorisation should not be granted for the use or conduct of a source unless believed that there are arrangements in place for ensuring there is at all times a person with the responsibility for maintaining a record of the authorisation and use made of source.

7.7 In deciding whether authorisation is required for a test purchase operation (for example in relation to sales of age restricted products), consideration should be given to:

- whether the activity is likely to result in the obtaining of private information about any person, and

- whether the test purchaser establishes or maintains a personal or other relationship with the seller.

In circumstances where the exercise is considered to fall outside the scope of RIPA, the reasons for this decision should be recorded.

7.8 An authorisation granted in writing by an Authorising Officer and approved by a Magistrates Court for the conduct or use of a CHIS will cease to have effect (unless renewed) at the end of a period of 12 months beginning with day on which it took effect.

7.9 Subject to legal privileged information, material obtained from a CHIS may be used as evidence in criminal proceedings whether these proceedings are brought by the Council or by another public authority.

7.10 Where the product of the use or conduct of a CHIS could be relevant to pending or future criminal or civil proceedings, it should be retained in accordance with applicable disclosure requirements.

7.11 Subject to legal privileged information, there is nothing under the Act which prevents material obtained from authorisations for the use or conduct of a CHIS for a particular purpose from being used to further other purposes.

7.12 When cancelling an authorisation, an Authorising Officer must ensure that proper arrangements have been made for the activity's discontinuance including directions for the management of the product.

7.13 An officer who conducts activity on the internet in such a way that they may interact with others, whether by publicly open websites or more private exchanges, in circumstances where the other parties could not reasonably be expected to know their true identity, should consider whether the activity requires a CHIS authorisation. A directed surveillance authorisation should also be considered, unless the acquisition of that information is or will be covered by the terms of an applicable CHIS authorisation.

<u>Collaborative Working</u>

8.1 When granting or applying for an authorisation, the officer will need to be aware of particular sensitivities in the local community where the surveillance or property interference is taking place, and of any similar activities being undertaken by other public authorities which could impact on the deployment of surveillance. It is therefore recommended that where an Authorising Officer considers that conflicts might arise, they should consult a senior officer within the police force area in which the investigation or operation is to take place.

8.2 Where possible, the Council should seek to avoid duplication of authorisations as part of a single investigation or operation. The Council may therefore work in conjunction with other agencies to carry out surveillance. It will not be necessary for each party to complete its own form of authorisation and the Council can rely upon a duly authorised form completed by another agency providing that the Authorising Officer and Legal Services are made aware and it has been approved by the Magistrates Court if required. Duplication of authorisations does not affect

the lawfulness of the activities to be conducted, but may create an unnecessary administrative burden on the Council.

8.3 A copy of the relevant forms and Magistrates Court approval should be obtained and copies kept in the same manner as an authorisation granted by the Council.

8.4 If an officer has any concerns regarding an authorisation, review or renewal completed by another agency they should refer the matter to Legal Services at the earliest opportunity.

Record Management

9.1 Authorising Officers must send the original of any authorisation, any cancellation, renewal or review to the SRO within 2 working days of the issue.

9.2 The Council must keep records relating to all authorisations, Magistrates Court approvals, reviews, renewals, cancellations and refusals in accordance with the Home Office Code of Practice. A Central Register of all authorisations, Magistrates approvals, reviews, renewals, cancellations, refusals and records of oral authorisations will be monitored and maintained by the SRO with each Department keeping their own file of copies of their authorisations.

9.3 Records must be available for inspection by the Investigatory Powers Commissioner and retained to allow the Investigatory Powers Tribunal to undertake its functions. Although records are only required to be retained for at least three years, it is therefore desirable, if possible, to retain records for up to five years. Such information will be reviewed at appropriate intervals to confirm that the justification for its retention is still valid and will be securely destroyed as soon as it is no longer needed for authorisation purposes.

9.4 There are separate and specific record keeping requirements where use is made of CHIS. Records 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 in the Council with responsibility for maintaining a record of the use made of the source.

9.5 Documents created under the RIPA procedure are highly confidential and shall be treated as such. Authorising Officers, through the Data Protection Officer must ensure compliance with the appropriate data protection requirements under the Data Protection Act 2018 and the Council's internal arrangements relating to the handling and storage of material. The procedures and safeguards outlined in the Home Office Code of Practice will also be applied in relation to the handling of any material obtained through directed surveillance. Any breaches of data protection requirements should be reported immediately to the Data Protection Officer.

9.6 The SRO will ensure that robust and adequate arrangements are in place for the secure handling, storage and destruction of material obtained through the use of surveillance. The Council's internal safeguards will be kept under periodic review to ensure that they remain up to date and effective. Where the material could be relevant to pending or future criminal proceedings, it should be retained in accordance with established disclosure requirements for a suitable period and subject to review.

General Considerations

10.1 The SRO will ensure that guidance and training on RIPA is provided to staff requiring it. A record of those receiving training will be kept by the SRO.

10.2 Complaints may be dealt with by means of the Council's Corporate Complaints procedure and/or by virtue of a complaint to the Investigatory Powers Tribunal (IPT) The IPT has jurisdiction to investigate and determine complaints against the Council's use of investigatory powers, and is the only appropriate tribunal for human rights claims against the intelligence services. Following receipt of a complaint or claim from a person, the IPT can undertake its own enquiries and investigations and can demand access to all information held by the Council necessary to establish the facts of a claim and to reach a determination.

10.3 The body responsible for the oversight of RIPA is the Investigatory Powers Commissioner (IPC). The IPC are authorised to carry out inspections of the Council to review intelligence gathering procedures and administration processes.

10.4 This Policy is a public document and is operational forthwith, replacing any previous policies and procedures. It will be reviewed from time to time by the SRO and the Council's Cabinet shall set this Policy annually to ensure that it remains fit for purpose.

10.5 Further advice on good practice is contained within the Home Office Codes of Practice as outlined at paragraph 1.2.

Appendix 1

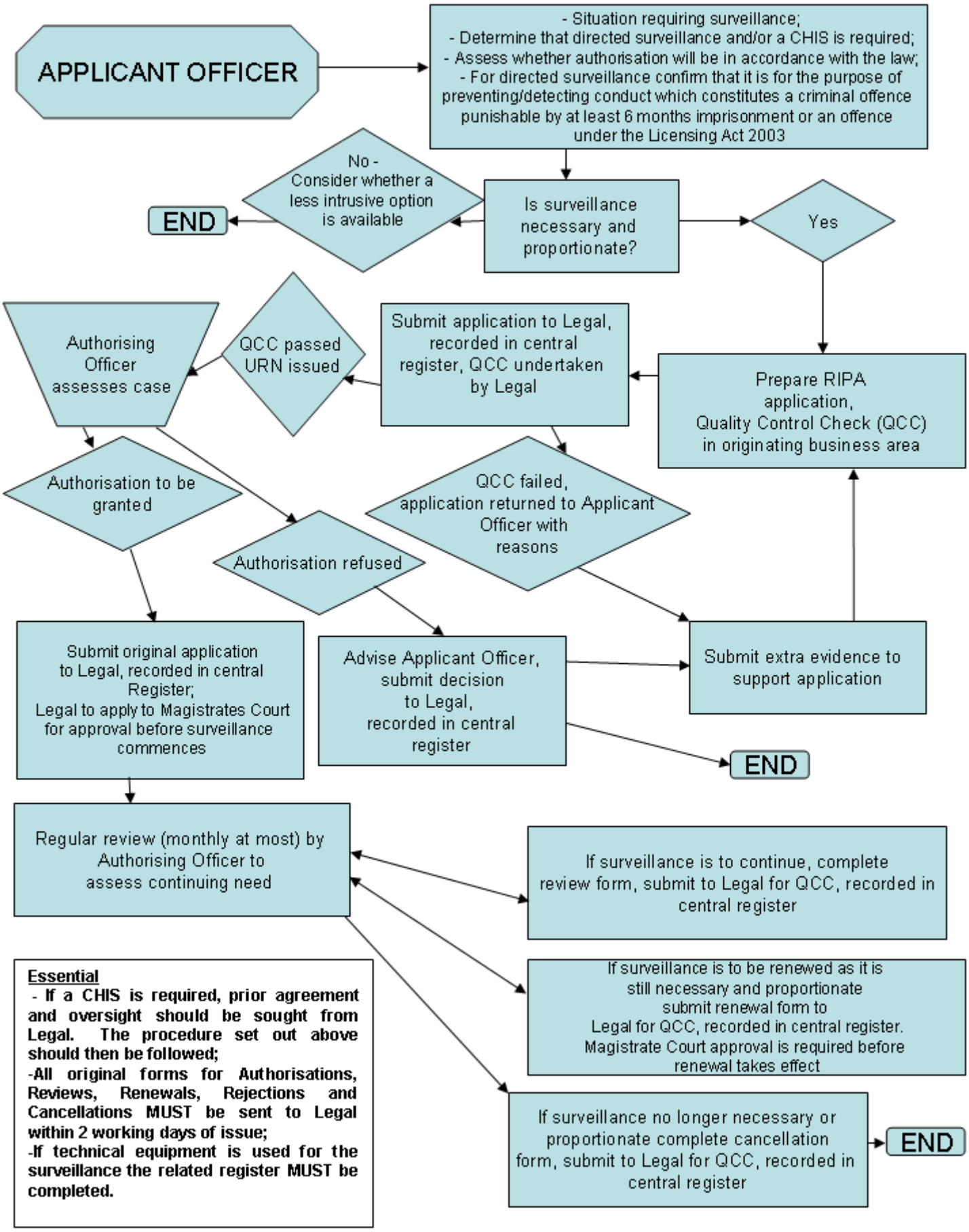
Senior Responsible Officer

The Monitoring Officer is authorised to act as the Senior Responsible Officer.

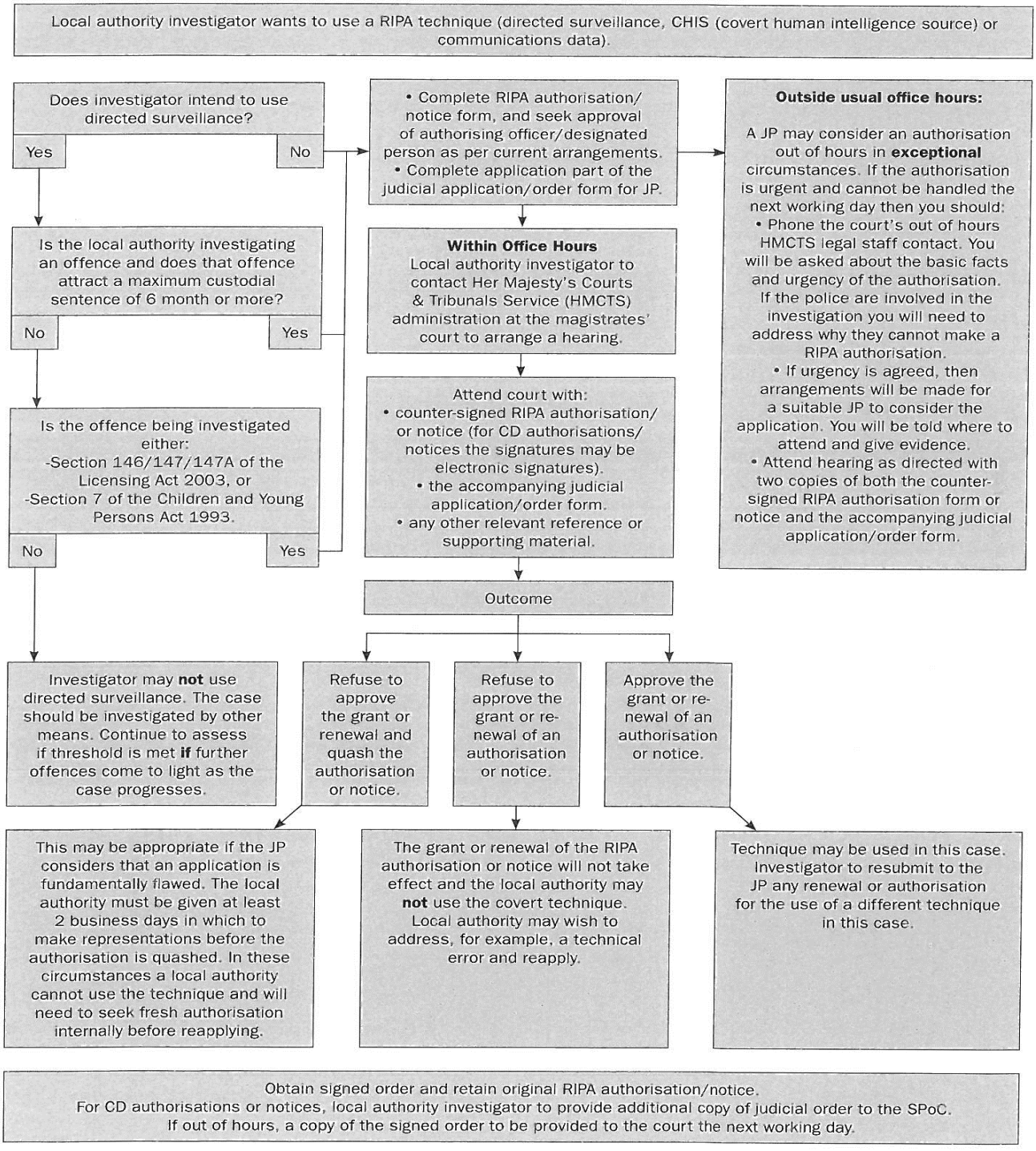
List of Designated Posts Nominated to Authorise Surveillance Activity in Bridgend County Borough Council under the Regulation of Investigatory Powers Act 2000.

Post	Directorate/Department
Chief Executive	Chief Executive
Head of Partnership Services	Chief Executive
Head of Operations – Community Services	Communities

RIPA AUTHORISATION FLOW CHART



LOCAL AUTHORITY PROCEDURE: APPLICATION TO A JUSTICE OF THE PEACE SEEKING AN ORDER TO APPROVE THE GRANT OF A RIPA AUTHORISATION OR NOTICE



17