NEATH PORT TALBOT COUNTY BOROUGH COUNCIL

REGULATION OF INVESTIGATORY POWERS ACT 2000

POLICY AND PROCEDURES

January 2024

CONTENTS

SECTION 1 – INTRODUCTION

1. Local Authorities powers to conduct covert surveillance come from the provisions of the Local Government Act 1972. The main restrictions on the use of those powers can be found in the Human Rights Act 1998, and in particular Article 8 of the European Convention on Human Rights (The right to respect for a person's private and family life).

2. The Regulation of Investigatory Powers Act 2000 (RIPA) (as amended) regulates covert investigations by a number of bodies, including local authorities. It was introduced to ensure that individuals' rights are protected whilst also ensuring that law enforcement and security agencies can still exercise the powers they need to do their job effectively. The Act only applies in relation to local authorities to any covert surveillance carried out by a local authority for the purposes of investigating qualifying criminal offences.

3. Covert surveillance carried out for reasons other than the investigation of qualifying criminal offences falls outside the scope of RIPA. Such surveillance can still be lawful, but extra care is needed to ensure such surveillance does not breach an individual's Human Rights. The purpose of this document is to set out the circumstances where RIPA applies to the Authority, and the procedures to be followed when conducting covert surveillance

4. Regard has been had to the respective Codes of Practice on Covert Surveillance & Property Interference and Covert Human Intelligence Sources issued by the Home Office in 2018, and Guidance and Practice notes issued by the Investigatory Powers Commissioner (IPCO) in preparing these procedures.

5. Subject to the provisions of Section 6 of this document, any covert surveillance activity carried out by or on behalf of the Council **MUST** be authorised by one of the properly trained Authorising Officers listed in Appendix 1, and dealt with in accordance with Section 5 of this document.

6. Individual Investigating Officers and Authorising Officers should familiarise themselves with this procedure document, the Codes of Practice issued by the Home Office, and such Guidance as is issued by the ICPO from time to time.

7. Deciding when an authorisation is required is a question of judgement. However, if an investigating officer is in any doubt, he/she should immediately seek legal advice from the Authority's Legal Services Section. **As a basic rule however, it is always safer to seek the appropriate authorisation.**

8. The Senior Responsible Officer within the Council with strategic responsibility for RIPA issues is Craig Griffiths, Head of Legal Services.

9. The 'Gate-keeping' Officer, with responsibility for vetting all RIPA applications and maintaining the Central register is Paul Watkins, Corporate Solicitor.

10. The elected members responsible for reviewing the authority's use of RIPA and setting the authority's RIPA policy each year are the Policy and Resources Cabinet Board.

11. All officers must note that the council may only authorise directed covert surveillance under the regulation of investigatory powers act for the purposes of preventing or detecting criminal offences that are punishable by a maximum term of at least 6 months imprisonment.

12. The only exception to the above rule is for the authorisation of test purchasing operations in relation to the sales of alcohol and tobacco or nicotine inhaling products to children.

13. The only exception to the above rule is for test purchasing operations in relation to the sale of alcohol or cigarettes to children.

14. Officers should also note that any surveillance which is carried out or authorised by them which does not comply with the requirements and/or stipulations of this policy may result in disciplinary action being taken against them by the council.

SECTION 2 - BENEFITS OF OBTAINING AUTHORISATION UNDER RIPA

1. RIPA states that where an authorisation is obtained, and the covert surveillance activity is conducted in accordance with that authorisation, then the activity will be lawful for all purposes.

2. Where an authorisation is not obtained, there is a risk that any evidence obtained as a result could be ruled as inadmissible in subsequent legal proceedings.

3. Furthermore, unauthorised covert surveillance activity is more likely to result in a breach of an individual's human rights, leading to a possible compensation claim against the Council.

SECTION 3 - DIRECTED SURVEILLANCE

1. Directed Surveillance includes;

    - The monitoring, observing or listening to persons, their movements, their conversations or their other activities or communication.

    - The recording of anything so monitored observed or listened to in the course of surveillance.

    - The surveillance by or with the assistance of a surveillance device.

2. Directed Surveillance does NOT occur where covert recording of suspected noise nuisance takes place and the recording device is calibrated to record only excessive noise levels.

3. Surveillance is ‘Directed’ for the purposes of RIPA if it is covert (but not intrusive) and is undertaken;

- For the purposes of a specific investigation into a criminal offence punishable by a maximum term of at least 6 months imprisonment, and
- In such a manner as is likely to result in the obtaining of private information about a person (whether or not one is specifically identified for the purposes of the investigation or operation); and

- Otherwise than by an immediate response to events or circumstances the nature of which is such that it would not be reasonably practicable for a Directed Surveillance authorisation to be sought for the carrying out of the surveillance

4. **OFFICERS SHOULD NOTE THAT THE SURVEILLANCE OF AN INDIVIDUAL’S ACTIVITIES AND/OR CONVERSATIONS IN *A* PUBLIC PLACE MAY STILL AMOUNT TO THE OBTAINING OF PRIVATE INFORMATION**

5. Surveillance is ‘covert’ if it is carried out in a manner calculated to ensure that the persons subject to the surveillance are unaware it is or may be taking place. Therefore surveillance of an individual using city centre CCTV cameras could still require RIPA authorisations if the cameras are targeted on that individual and he/she is unaware that they are being watched.

6. Covert surveillance becomes ‘intrusive’ if;

(a) It is carried out in relation to anything taking place on any residential premises or in any private vehicle or on premises where legal consultations are taking place, and

(b) Involves the presence of an individual on the premises or in the vehicle or is carried out by means of a surveillance device on the premises or in the vehicle, or

(c) Is carried out by means of a surveillance device in relation to anything taking place on any residential premises or in any private vehicle but is carried out without that device being on the premises or in the vehicle or legal consultation premises, where the device is such that it consistently provides information of the same quality and detail as might be expected to be obtained from a device actually present on the premises or vehicle.

(d) For the purposes of (a), (b) and (c) above 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.

7. <u>THE COUNCIL HAS NO POWER TO AUTHORISE INTRUSIVE SURVEILLANCE UNDER THE ACT. IF INVESTIGATING OFFICERS HAVE ANY CONCERNS REGARDING THIS THEY SHOULD IMMEDIATELY SEEK LEGAL ADVICE.</u>

8. Surveillance is for the purposes of a specific investigation or operation if it is targeted in a pre-planned way at an individual or group of individuals, or a particular location or series of locations.

9. Surveillance will not require authorisation if it is by way of an immediate response to an event or circumstances where it is not reasonably practicable to get an authorisation.

SECTION 4 - COVERT HUMAN INTELLIGENCE SOURCES (CHIS)

1. A person is a CHIS if;

   - He/she establishes or maintains a personal or other relationship with a person for the covert purpose of facilitating the doing of anything falling within paragraphs (a) or (b) below.

     (a) He/she covertly uses such a relationship to obtain information or provide access to any information to another person, or

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

2. Guidance to Local Authorities on who may or may not be a CHIS is set out in the Covert Human Intelligence Sources Code of Practice produced by the Home Office. The relevant extracts from that guidance are set out in Appendix 8 below for officers' information.

3. A purpose is covert in this context if the relationship is conducted in a manner that is calculated to ensure that one of the parties is unaware of that purpose.

4. Council policy is to treat all such activities as being in need of authorisation whether or not the information sought is private information.

5. When considering whether or not to make use of CHIS, investigating officers ***MUST*** consult with the gate-keeping officer before taking any action, in order to ensure that the Home Office Code of Practice on Covert Human Intelligence Sources is complied with. Where use is made of CHIS, his/her designated handler must be a properly trained officer, who may not necessarily be based within the same department/section as the investigating officer.

6. It is the intention of this Council to avoid the use of a CHIS whenever possible; accordingly any contemplated use must be discussed with the Head of Legal Services in all cases.

7. Only the Chief Executive may authorise the use of a juvenile CHIS.

8. THIS AUTHORITY DOES NOT CONDONE THE USE OF A JUVENILE AS A CHIS. ACCORDINGLY, NO CHIS SHALL BE AUTHORISED IN RESPECT OF A PERSON UNDER 18 YEARS OF AGE BY ANY AUTHORISING OFFICERS.

SECTION 5 - AUTHORISATION PROCESS

1. Applications must be in writing, using the standard forms provided by the Home Office. A list of these forms are set out in Appendix 2 and are available for downloading from the Home Office website by entering “RIPA Forms” in its search engine.

2. Although it is possible to combine two or more applications in the same form, this practice is generally to be avoided. One situation where it may be appropriate is during a covert test purchase exercise involving more than one premise. In such cases investigating officers should contact the gate-keeping officer to discuss the operation before completing the forms.

3. Once the appropriate application forms are completed, they should be submitted by email to the gate-keeping officer.

4. The gate-keeping officer will then vet the application, enter it onto the Central Register and allocate a unique central reference number (URN) to it.

5. The gate-keeping officer may recommend changes to the application, or agree to it being submitted unaltered to a designated Authorising Officer. A list of such officers is set out in Appendix 1.

6. Where an application must be authorised by the Chief Executive (i.e. in cases of a juvenile CHIS or confidential information), the gate-keeping officer will arrange a meeting

between the Investigating Officer, Head of Legal Services and Chief Executive.

7. In all other cases the investigating officer shall arrange to meet one of the Authorising Officers to discuss the application.

8. When determining whether or not to grant an authorisation, Authorising Officers must have regard to;

- Whether what is proposed is necessary for preventing/detecting criminal offences that meet the requirements in Section 1 paragraphs 11 and 12 above.

- Whether what is proposed is proportionate to the aim of the action

- 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.

- 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.

    - Whether the proposed action is likely to result in collateral intrusion into the private lives of third parties, and if it is, whether all reasonable steps are being taken to minimise that risk.

- 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.

- In the case of applications to authorise the use of a CHIS, whether all the requirements of the Code of Practice relating to the authorisation of a CHIS issued by the Home Office are complied with.

9. If an application is refused by an Authorising officer, the reasons for refusal shall be endorsed on the application form.

10. If an application is granted, the Authorising Officer must specify;

- The scope of the authorisation

- The duration of the authorisation

- The date (not more than one month) for review of the authorisation.

11. Irrespective of the outcome of the application, the investigating officer must immediately forward the authorisation or refused application, to the gate-keeping officer, who will make the appropriate entries in the Central

Register, and place the application or authorisation in the Central Record.

12. Legal Services Section will then arrange for an application to be made to the Magistrates Court for the judicial approval of the authorisation. The procedure for such an application for approval is set out in Appendix 3.

13. **ALL OFFICERS MUST NOTE THAT THE AUTHORISATION WILL NOT TAKE EFFECT UNTIL IT HAS BEEN JUDICIALLY APPROVED BY MAGISTRATES COURT.**

14. If, upon initial review of the authorisation, the Authorising Officer determines that it should remain in effect, reviews must take place monthly during the life of the authorisation. The investigating officer must keep a record of the results of any review and communicate them to the gate-keeping officer for entry in the Central Register.

15. Once the operation to which the authorisation relates is concluded, or the activity authorised ceases, then the investigating officer must immediately meet the Authorising Officer to cancel the authorisation.

16. Once an Authorising Officer determines that an authorisation is no longer necessary it must be cancelled immediately.

17. Although paragraph 5.18 of the Covert Surveillance and Property Interference Code of Practice is correct in saying that there is no *requirement* for any further details to be recorded when cancelling a directed surveillance authorisation, the Commissioners consider that it would be sensible to complete the authorisation process in a form similar to other parts of the authorisation where relevant details can be retained together. When cancelling an authorisation, the Authorising Officer should:
    - Record the date and times (if at all) that surveillance took place and the order to cease the activity was made.
    - The reason for cancellation.
    - Ensure that surveillance equipment has been removed and returned.
    - Provide directions for the management of the product.

- Ensure that detail of property interfered with, or persons subjected to surveillance, since the last review or renewal is properly recorded.
- Record the value of the surveillance or interference (i.e. whether the
  objectives as set in the authorisation were met).

18. Whenever an authorisation is cancelled, a copy of that cancellation must be sent to the gate-keeping officer for it to be placed in the Central Record, and appropriate entries to be made in the Central Register.

19. Unless previously cancelled, an authorisation will last as follows:

    - Written authorisation for Directed Surveillance – **3 months**

    - Written authorisation for use of a CHIS – **12 months**

20. If shortly before an authorisation ceases to have effect, the Authorising Officer is satisfied that the grounds for renewing the authorisation are met, then he/she may renew the authorisation by completing a renewal form. ***(Before renewing an authorisation, Authorising Officers must have regard to the appropriate sections of the relevant code of practice issued by the Home Office)***

21. An authorisation may be renewed for;

    - In the case of a written renewal of a Directed Surveillance authorisation - **3 Months**.

    - In the case of a written renewal of a CHIS authorisation – **12 months**.

22. An authorisation may be renewed more than once.

23. Applications for renewal of an authorisation must record all matters required by the relevant Code of Practice issued by the Home Office

24. Where an authorisation is renewed, it must continue to be reviewed in accordance with the requirements set out above.

25. Where an authorisation is renewed, a copy of the renewal must be sent to the gate-keeping officer and placed in the Central Record and appropriate entries made in the Central Register.

26. Legal Services Section will then arrange for an application to be made to the local magistrates' court for the judicial approval of the renewal by a Magistrate.

27. **ALL OFFICERS MUST NOTE THAT THE RENEWAL WILL NOT TAKE EFFECT UNTIL IT HAS BEEN JUDICIALLY APPROVED BY A MAGISTRATE.**

28. **WHERE AN APPLICATION IS GRANTED OR RENEWED THE INVESTIGATING OFFICER MUST ENSURE THAT ALL OFFICERS TAKING PART IN THE COVERT SURVEILLANCE ACTIVITY HAVE AN OPPORTUNITY TO READ THE AUTHORISATION AND FAMILIARISE THEMSELVES WITH ITS TERMS AND RESTRICTIONS BEFORE THE OPERATION COMMENCES *(ruling established in R -v- Sutherland).***

SECTION 6 - COVERT SURVEILLANCE AUTHORISED OUTSIDE RIPA

1. Certain instances of covert surveillance that may be carried out by public authorities are incapable of being authorised under RIPA. Examples of these include:

- The investigation of criminal offences punishable by less than 6 months imprisonment.

- The investigation of general disorder or anti-social behaviour.

- Surveillance carried out as part of a planning investigation prior to issuing an enforcement notice

- Surveillance carried out as part of a public health investigation prior to issuing an abatement notice.

- Surveillance carried out as part of an internal disciplinary, child protection or POVA investigation.

- Surveillance carried out in support of the defence of a personal injury claim

- The use of surveillance devices to monitor a person living in a residential care setting where it is considered to be in their 'best interests' to do so.

2. None of these examples can be authorised as directed surveillance under RIPA, although all are capable of being justifiable cases of interference with an individual's human rights on the grounds that they are necessary in a democratic society in the interests of public safety, the economic well-being of the country, for the protection of health or morals or for the protection of rights and freedoms of others. In these cases, although the authority cannot rely upon RIPA to authorise surveillance, such surveillance can still be carried out provided steps are undertaken to ensure any interference with an individual's human rights complies with the requirements set out in Article 8 of the European Convention on Human rights.

3. Wherever an officer wishes to consider carrying out directed surveillance, which cannot be justified on the grounds in RIPA, but which may fall within the scope of paragraphs 1 and 2 above, he/she should contact the Authority's Legal Services Section for advice.

4. **NO SURVEILLANCE ACTIVITY OF THE SORT OUTLINED IN PARAGRAPH 1 ABOVE MAY TAKE PLACE UNLESS IT HAS BEEN EXPRESSLY APPROVED IN WRITING BY THE INVESTIGATING OFFICER'S HEAD OF SERVICE.**

SECTION 7 - CONFIDENTIAL MATERIAL

1. Confidential material such as personal medical or spiritual information, confidential journalistic information, information between an MP and his/her constituent or information

subject to legal privilege is particularly sensitive and is subject to additional safeguards.

2. In cases where such information may be obtained, an investigator must seek immediate legal advice from the Authority's Legal Services Section.

3. **Only the Chief Executive may authorise surveillance activity which may result in confidential information being obtained.**

4. Any application for an authorisation, which is likely to result in the acquisition of confidential material MUST include an assessment of how likely it is that confidential material will be acquired.

5. Special care should be taken where the target of the investigation is likely to be involved in handling confidential material. Such applications should only be considered in exceptional and compelling circumstances and with full regard to the proportionality issues this raises.

6. The following general principles apply to confidential material acquired under such authorisations;

   - Officers handling material from such operations should be alert to anything that may fall within the definition of confidential material. Where there is any doubt, immediate legal advice should be sought.

   - Confidential material should not be retained or copied unless it is necessary for a specified purpose.

   - Confidential material should only be disseminated, after legal advice has been sought, where it is necessary for a specified purpose.

   - The retention and/or dissemination of confidential material should be accompanied by a clear warning of its confidential nature.

- Confidential material should be destroyed as soon as it is no longer necessary to retain it for a specified purpose.

SECTION 8 - JOINT OPERATIONS

1. Where officers are engaged in operations with other public authorities, any covert activity must be authorised either in accordance with this document, or by an appropriate Authorising Officer employed by the other authority.

2. Officers should always ensure that when operating under an authorisation issued by another authority, that the Authorising Officer has the power to issue that authorisation, and that the authorisation covers the scope of the proposed activity.

3. Officers are advised to request a copy of the relevant authorisation, or at least obtain a written note of the scope, duration and conditions of the authorised activity.

4. Officers should also have regard to any other protocols specifically dealing with joint operations.

SECTION 9 - HANDLING & DISCLOSURE OF PRODUCT

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.

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.

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.

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.

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. Any breaches of data protection requirements should be reported immediately to the Data Protection Officer.

6. The procedures and safeguards outlined in the Home Office Covert Surveillance and Property Interference Code of Practice in **and** the Covert Human Intelligence Sources Code of Practice respectively in regards to the dissemination, copying, storage and destruction of any material obtained through covert surveillance and/or the use of a Covert Human Intelligence Source must also be applied in relation to the handling and storage of material. Extracts from the above respective Codes are set out in Appendices 6 and 7 below.

7. 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.

8. Where material is obtained by surveillance, which is wholly unrelated to a criminal or other investigation or to any person who is the subject of such an investigation, and there is no reason to believe it will be relevant to future criminal or civil proceedings, it should be destroyed immediately.

9. Consideration as to whether or not unrelated material should be destroyed is the responsibility of the Authorising Officer.

10. RIPA does not prevent material properly obtained in one investigation being used in another investigation. **However, the use of any covertly obtained material for purposes other than that for which the surveillance was authorised should only be sanctioned in exceptional cases and only after seeking legal advice from the Council's Legal Services Section.**

SECTION 10 - USE OF SURVEILLANCE DEVICES

1. Surveillance devices include static and mobile CCTV cameras, covert surveillance cameras, noise monitoring/recording devices, and any other mechanical and/or recording devices used for surveillance purposes.

2. Static CCTV cameras include 'Town Centre' cameras operated from the authority's CCTV Control Room under the control of Council staff, as well as fixed security cameras located in council buildings.

3. Fixed security cameras, which are incapable of being remotely controlled, do not require RIPA authorisation ***provided*** their existence and purpose is made clear to the public through appropriate signage.

4. ‘Town Centre’ and mobile CCTV cameras will not ordinarily require authorisation where their existence and use is also made clear by signage. However, where camera operators are requested to control the cameras so as to target specific individuals or locations then, unless the request is made by way of an immediate response to an incident or intelligence received, an authorisation is required.

5. Camera operators should normally refuse to comply with any requests for surveillance activity unless they are satisfied;

   - That an authorisation is unnecessary, or

   - That an authorisation has been obtained and the scope, duration and limitations of the permitted activity have been confirmed in writing.

6. It is recognised that many departments maintain conventional cameras and mobile phone cameras for use by staff on a regular basis. Staff must be reminded;

   - That the covert use of such cameras (i.e. where the ‘target’ is not aware that he/she is being photographed) may require authorisation.

   - As a general rule, unless the photograph is being taken as an immediate response to an unexpected incident, authorisation should be sought.

7. Use of noise monitoring/recording equipment may also require authorisation, where the equipment records actual noise, as opposed to just noise levels. Much will depend upon what noise it is intended, or likely, to record.

8. Where a target is made aware in writing that noise monitoring will be taking place, then authorisation is not required.

9. Service Managers with responsibility for surveillance devices **MUST** ensure that:

(i) Those devices are stored securely and that robust systems are in place to prevent unauthorised access to them both by Council staff and members of the public.

(ii) Full and accurate records are kept at all times documenting the use of those devices including (but not limited to), when deployed, the purpose of any deployment, the officer with responsibility for that deployment and, where being deployed to conduct Directed Surveillance, details of any authorisation under which that deployment takes place

(iii) Any personal information obtained as a result of the deployment of such a device is handled in accordance with the Council's Data Protection Policies.

SECTION 11 – COVERT SURVEILLANCE OF SOCIAL NETWORKING SITES

1. Care must be taken when using or monitoring a Social Networking Site for work purposes. Even though a site may seem to be an open source of publically available information, the author may have expectations of privacy, especially if they apply at least some access controls.

2. The fact that digital investigation is routine or easy to conduct does not reduce the need for authorisation. Care must be taken to understand how the Social Networking Site is being used works, Authorising 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.

3. Whilst it is the responsibility of an individual to set privacy settings to protect unsolicited access to private information, and even though data may be deemed published and no longer under the control of the author, it is unwise to regard it as "open source" or publicly available; the author has a reasonable expectation of privacy if access controls are applied. Where privacy settings are available but not applied the data may be considered open source and an authorisation is not usually required. Repeat viewing of "open source" sites may constitute directed surveillance on a case by case basis and this should be borne in mind.

4. If it is necessary and proportionate for a public authority to covertly breach access controls, the minimum requirement is an authorisations for Directed Surveillance. An authorisation for the use and conduct of a CHIS is necessary if a relationship is established or maintained by a member of a public authority or by a person acting on its behalf (i.e. the activity is more than mere reading of the site's content).

5. It is not unlawful for a member of a public authority to set up a false identity but it is inadvisable for a member of a public authority to do so for a covert purpose without authorisation. Using photographs of other persons without their permission to support the false identity infringes other laws.

6. 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 identify is used, and without considering the protection of that person. The consent must be explicit (.i.e. the person from whom consent is sought must agree (preferably in writing) what is and is not to be done).

7. Any use of a Social Networking Site for these purposes must also comply with Council policies on Internet and Social Media Usage which can be found on the Authority's Intranet.

8. Appendices 4 and 5 set out the guidance in the Code of Practices for Covert Surveillance and Property Interference and Covert Human Intelligence Sources respectively which deal with the use of social media.

SECTION 12 - CODES OF PRACTICE

1. The Home Office has issued Codes of Practice relating both to Covert Surveillance and the use of CHIS. Copies of these codes are available via the Home Office, or ICPO websites, or can be obtained from the gate-keeping officer.

2. These codes are statutory guidance, and adherence to them will give the authority a better chance of opposing any

allegation that RIPA and/or the Human Rights Act has been breached by its use of covert surveillance.

3. Investigating and Authorising Officers should ensure that when dealing with applications, regard is had to these codes.

4. The Investigatory Powers Commissioner has also published useful guidance, copies of which can be obtained from his website or the gate-keeping officer.

SECTION 13 - SCRUTINY AND TRIBUNAL

The council will be subject to an inspection by an OSC inspector roughly every 2 years. The inspector will;

- Examine the Central Register
- Examine authorisations, renewals and cancellations
- Question officers regarding their implementation of the legislation.
- Report to the Chief Executive regarding his/her findings

A Tribunal has also been set up to deal with complaints made under RIPA. The Tribunal may quash or cancel any authorisation and order the destruction of any record or information obtained as a result of such an authorisation.

Courts and Tribunals may exclude evidence obtained in breach of an individual's human rights. Failure to follow the procedures set out in this document increases the risk of this happening.

This document will be kept under annual review by the Council's Cabinet, who will also receive regular reports as to its implementation.

SECTION 14 – TRAINING

The Senior Responsible Officer will ensure that guidance and/or training is being provided to investigating and/or authorising officer as and when necessary to ensure that RIPA is being used

appropriately. A record of officers training will be maintained by the relevant investigating departments within the Council; which shall be made available to the Senior Responsible Officer as and when he requires them for his monitoring purposes.

APPENDIX 1

LIST OF AUTHORISING OFFICERS

Name	Post
Karen Jones	Chief Executive
Michael Roberts	Head of Streetcare
Nicola Pearce	Director of Environment and Regeneration
Ceri Morris	Head of Planning and Public Protection

APPENDIX 2

PART II OF THE REGULATION OF INVESTIGATORY POWERS ACT 2000 – HOME OFFICE FORMS

1. Authorisation of Directed Surveillance.
   (Version: 2010-09 DS Application)

2. Review of a Directed Surveillance Authorisation
   (Version: 2007-01 DS Review)

3. Renewal of a Directed Surveillance Authorisation

(Version: 2007-01 DS Renewal)

4. Cancellation of a Directed Surveillance Authorisation
(Version: 2007-01 DS Cancellation)

5. Application for Authorisation of the Conduct or Use of a Covert Human Intelligence Source (CHIS)
(Version: 2010-09 CHIS Application)

6. Review of a Covert Human Intelligence Source (CHIS) Authorisation
(Version: 2010-09 CHIS Review)

7. Application for a Renewal of a Covert Human Intelligence Source (CHIS) Authorisation
(Version: 2007-01 CHIS Renewal)

8. Cancellation of an Authorisation of the Use or Conduct of a Covert Human Intelligence Source
(Version: 2007-01 CHIS Cancellation)

APPENDIX 3

COUNCIL PROCEDURE FOR APPLYING TO A MAGISTRATES COURT FOR AN AUTHORISATION TO BE APPROVED BY A JUSTICE OF THE PEACE AND APPLICATION FORM TO BE USED

1. Complete the usual RIPA directed surveillance or telecoms application form, providing full details for the necessity and proportionality issues.

2. Have the RIPA form approved by an Authorised Officer in the Council.

3. Complete a new ‘Approval by a Justice of the Peace’ application form.

4. Contact Legal Services to seek availability of a Solicitor or Barrister to attend court.

5. Contact office at Magistrates Court to book an appointment with a JP.

6. Attend court accompanied by a solicitor to make the application with JP.

7. If RIPA is approved and supported by a JP they will sign the Order, which is the 2nd page of the 'Approval by JP' form (see attached).

Then….

8. RIPA application to be reviewed by the Authorised Officer with the investigator every month, to review its continued necessity and proportionality.

9. After 3 months the initial RIPA authorisation will come to an end. It will then need to be (i) cancelled or (ii) renewed – and the necessary forms completed.

10. There is no requirement for a JP to be involved in RIPA reviews and/or cancellations as this is merely an internal process.

11. If a RIPA application is to be renewed – continued past 3 months – then a JP will once again need to be involved. The investigator will need to complete a RIPA Renewal form and then follow points 2 to 6 above again, seeking a signed Order from a JP at court.

REGULATION OF INVESTIGATORY POWERS ACT 2000

APPLICATION FOR APPROVAL BY A JUSTICE OF THE PEACE

Application for judicial approval for authorisation to use a covert human intelligence source or to conduct directed surveillance. Regulation of Investigatory Powers Act 2000 sections 32A, 32B.

Local authority: Neath Port Talbot County Borough Council
Local authority department: ……..
Offence under investigation: …….

Address of premises or identity ……..
……...
…….

Covert technique requested: (tick one and specify details)

Covert Human Intelligence Source ☐

Directed Surveillance ☐

Summary of details

……
……
……
……
……
……

Note: this application should be read in conjunction with the attached RIPA authorisation/RIPA application or notice.

Investigating Officer: ……
Authorising Officer/Designated Person: ……...
Officer(s) appearing before JP: …….
Address of applicant department: …….
……
Contact telephone number: ……
Contact email address (optional): ……
Local authority reference: ……
Number of pages: …….

ORDER

Order made on an application for judicial approval for authorisation to use a covert human intelligence source or to conduct directed surveillance. Regulation of Investigatory Powers Act 2000 sections 32A and 32B.

Magistrates' court: Swansea Magistrates Court

Having considered the application, I (tick one):

☐ am satisfied that there are reasonable grounds for believing that the requirements of the Act were satisfied and remain satisfied, and that

the relevant conditions are satisfied and I therefore approve the grant or renewal of the authorisation / notice.

☐ refuse to approve the grant or renewal of the authorisation /notice.

☐ refuse to approve the grant or renewal and quash the authorisation/notice.

Notes

……
……
……
……
……

Reasons

……
……
……
……
……
……
……

Signed:

Date:

Time:

Full name:

Address of magistrates' court: Grove Place, Swansea, SA1 5DB

APPENDIX 4

Social Media – Extract from Home Office Code of Practice on Covert Surveillance and Property Interference (3.10 to 3.17)

3.10 The growth of the internet, and the extent of the information that is now available online presents new opportunities for public authorities to view or gather information which may assist them in preventing or detecting crime or carrying out other statutory functions, as well as in understanding and

engaging with the public they serve. It is important that public authorities are able to make full and lawful use of this information for their statutory purposes. Much of it can be accessed without the need for RIPA authorisation; use of the internet prior to an investigation should not normally engage privacy considerations. But 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. The following guidance is intended to assist public authorities in identifying when such authorisations may be appropriate.

3.11 The internet may be used for intelligence gathering and/or as a surveillance tool. Where online monitoring or investigation is conducted covertly for the purpose of a specific investigation or operation and is likely to result in the obtaining of private information about a person or group, an authorisation for directed surveillance should be considered, as set out elsewhere in this code. Where a person acting on behalf of a public authority is intending to engage with others online without disclosing his or her identity, a CHIS authorisation may be needed (paragraphs 4.10 to 4.16 of the Covert Human Intelligence Sources code of practice provide details on where a CHIS authorisation may be available for online activity).

3.12 In deciding whether online surveillance should be regarded as covert, consideration should be given to the likelihood of the subject(s) knowing that the surveillance is or may be taking place. Use of the internet itself may be considered as adopting a surveillance technique calculated to ensure that the subject is unaware of it, even if no further steps are taken to conceal the activity. Conversely, where a public authority has taken reasonable steps to inform the public or particular individuals that the surveillance may be taking place, the activity may be regarded as overt and a directed surveillance authorisation will not normally be available.

3.13 As set out in paragraph 3.14 below, 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 an 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.

3.14 Where information about an individual is placed on a publicly accessible database, for example the telephone directory or Companies House, which is commonly used and known to be accessible to all, they are unlikely to have any reasonable expectation of privacy over the monitoring by public authorities of that information. Individuals who post information on social media networks and other websites whose purpose is to communicate messages to a wide audience are also less likely to hold a reasonable expectation of privacy in relation to that information.

3.15 Whether a public authority interferes with a person's private life includes a consideration of the nature of the public authority's activities in relation to that information. Simple reconnaissance of such sites (i.e. preliminary examination with a view to establishing whether the site or its contents are of interest) is unlikely to interfere with a person's reasonably held expectation of privacy and therefore is not likely to require a directed surveillance authorisation. But where a public authority is systematically collecting and recording information about a particular person or group, a directed surveillance authorisation should be considered. These considerations apply regardless of when the information was shared online. See also paragraph 3.6

Example 1

A police office undertakes a simple internet search on a name, address and 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 identify, 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

A customs office makes an initial examination of an individual's online profile to establish whether they are of relevance to an investigation. This is unlikely to need an authorisation. However, if during that visit it is intended to extract and record information to establish a profile including information such as identify, pattern of life, habits, intentions or associations, it may be advisable to have in place an authorisation even for that single visit. (As set out in the following paragraph, the purpose of the visit may be relevant as to whether an authorisation should be sought.)

Example 3

A public authority 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.

3.16 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 or organisation;
- Whether it is likely to result in obtaining private information about a person or group or people (taking account of the guidance at paragraph 3.6 above)

- Whether it is likely to involve visiting internet sites to build up an intelligence 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 or intelligence, 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.

3.17 Internet searches carried out by a third party on behalf of a public authority, or with the use of a search tool, may still require a directed surveillance authorisation (see paragraph 4.32)

Example
Researches within a public authority using automated monitoring tools to search for common terminology used online for illegal purposes will not normally require a directed surveillance authorisation. Similarly, general analysis of data by public authorities either directly or through a third party for predictive purposes (e.g. identifying crime hotspots or analysis trends) is not usually directed surveillance. In such cases, the focus on individuals or groups is likely to be sufficiently cursory that it would not meet the definition of surveillance. But officers should be aware of the possibility that the broad thematic research may evolve, and that authorisation may be appropriate at the point where it begins to focus on specific individuals or groups. If specific names or other identifies of an individual or group are applied to the search or analysis, an authorisation should be considered.

Appendix 5
Social Media – Extract from Home Office Code of Practice on Covert Human Intelligence Sources (4.29-4.35)

4.29 Any member of a public authority, or person acting on their behalf, who conducts activity on the internet in such a way that they may interact with others 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. This applies whether the interaction involves publicly open websites such as an online news and social networking service, or more private exchanges such as messaging sites. Where the activity is likely to result in obtaining private information but does not amount to establishing or maintaining a CHIS relationship, consideration should be given to the need for a directed surveillance authorisation.

4.30 Where someone, such as an employee or member of the public, is tasked by a public authority to use an internet profile to establish or maintain a relationship with a subject of interest for a covert purpose, or otherwise undertakes such activity on behalf of the public authority, in order to obtain or provide access to information, a CHIS authorisation is likely to be required. For example:

- an investigator using the internet to engage with a subject of interest at the start of an operation, in order to ascertain information or facilitate a meeting in person;
- directing a member of the public to use their own or another internet profile to establish or maintain a relationship with a subject of interest for a covert purpose;
- joining chat rooms with a view to interacting with a criminal group in order to obtain information about their criminal activities.

4.31 A CHIS authorisation will not always be appropriate or necessary for online investigation or research. Some websites require a user to register providing personal identifiers (such as name and phone number) before access to the site will be permitted. Where a member of a public authority sets up a false

identity for this purpose, this does not in itself amount to establishing a relationship, and a CHIS authorisation would not immediately be required. However, consideration should be given to the need for a directed surveillance authorisation if the conduct is likely to result in the acquisition of private information, and the other relevant criteria are met.

Example 1: An HMRC officer intends to make a one-off online test purchase of an item on an auction site, to investigate intelligence that the true value of the goods is not being declared for tax purposes. The officer concludes the purchase and does not correspond privately with the seller or leave feedback on the site. No covert relationship is formed, and a CHIS authorisation need not be sought.

Example 2: HMRC task a member of the public to purchase goods from a number of websites to obtain information about the identity of the seller, country of origin of the goods and banking arrangements. The individual is required to engage with the seller as necessary to complete the purchases. The deployment should be covered by a CHIS authorisation because of the intention to establish a relationship for covert purposes.

4.32 Where a website or social media account requires a minimal level of interaction, such as sending or receiving a friend request before access is permitted, this may not in itself amount to establishing a relationship. Equally, the use of electronic gestures such as “like” or “follow” to react to information posted by others online would not in itself constitute forming a relationship. However, it should be borne in mind that entering a website or responding on these terms may lead to further interaction with other users and a CHIS authorisation should be obtained if there is an intention to engage in such interaction to obtain, provide access to or disclose information.

Example 1: An officer maintains a false persona, unconnected to law enforcement, on social media sites in order to facilitate future operational research or investigation. As part of the legend building activity he “follows” a variety of people and entities and “likes” occasional posts without engaging further. No relationship is formed, and no CHIS authorisation is needed.

Example 2: An officer who has maintained a false persona uses that persona to send a request to join a closed group known to be administered by a subject of interest, connected to a specific investigation. A directed surveillance authorisation would be likely to be appropriate in respect of the proposed covert monitoring of the site if the activity is likely to result in obtaining private information. Once accepted into the group it becomes apparent that further interaction is necessary: this should be authorised by means of a CHIS authorisation.

4.33 When engaging in conduct as a CHIS, 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 considering the need for a CHIS authorisation. Full consideration should be given to the potential risks posed by that activity.

4.34 Where use of the internet is part of the tasking of a CHIS, the risk assessment carried out in accordance with paragraphs 7.15 to 7.21 of this Code should include consideration of the risks arising from that online activity including factors such as the length of time spent online and the material to which the CHIS may be exposed. This should also take account of any disparity between the technical skills of the CHIS and those of the handler or Authorising Officer, and the extent to which this may impact on the effectiveness of oversight.

4.35 Where it is intended that more than one person will share the same online persona, each individual should be clearly identifiable within the overarching authorisation for that operation. The authorisation should provide clear information about the conduct required of – and the risk assessments in relation to – each individual involved.

Appendix 6
Covert Surveillance and Property Interference
Code of Practice
(Sections 9.5, 9.16 – 9.22 – Dissemination, Copying, Storing and Destruction of Materials)

9.5 Dissemination, copying and retention of material must be limited to the minimum necessary for authorised purposes. For the purposes of this code, something is necessary for the authorised purposes if the material:

- is, or is likely to become, necessary for any of the statutory purposes set out in the 2000, 1997 or 1994 Act in relation to covert surveillance or property interference;
- is necessary for facilitating the carrying out of the functions of public authorities under those Acts;
- is necessary for facilitating the carrying out of any functions of the Commissioner or the Investigatory Powers Tribunal;
- is necessary for the purposes of legal proceedings; or
- is necessary for the performance of the functions of any person by or under any enactment.

Dissemination of Information

9.16 Material acquired through covert surveillance or property interference will need to be disseminated both within and between public authorities, as well as to consumers of intelligence (which includes oversight bodies and the Secretary of State, for example), where necessary in order for action to be taken on it. The number of persons to whom any of the information is disclosed, and the extent of disclosure, should be limited to the minimum necessary for the authorised purpose(s) set out in 9.5 above. This obligation applies equally to disclosure to additional persons within a public authority and to disclosure outside the authority. In the same way, only so much of the material may be disclosed as the recipient needs; for example if a summary of the material will suffice, no more than that should be disclosed.

9.17 The obligations apply not just to the original public authority acquiring the information under a warrant or authorisation, but also to anyone to whom the material is subsequently disclosed. In

some cases, this will be achieved by requiring the latter to obtain the original authority's permission before disclosing the material further. In others, explicit safeguards should be applied to secondary recipients.

9.18 Where material obtained under a warrant or authorisation is disclosed to the authorities of a country or territory outside the UK, the public authority must ensure that the material is only handed over to the authorities if it appears to them that any requirements relating to minimising the extent to which material is disclosed, copied, distributed and retained will be observed to the extent that the authorising officer, Judicial Commissioner or Secretary of State considers appropriate.

Copying

9.19 Material obtained through covert surveillance or property interference may only be copied to the extent necessary for the authorised purposes set out at 9.5 above. Copies include not only direct copies of the whole of the material, but also extracts and summaries which identify themselves as the product of covert surveillance or property interference, and any record which refers to the covert surveillance or property interference and the identities of the persons to whom the material relates.

Storage

9.20 Material obtained through covert surveillance or property interference, and all copies, extracts and summaries of it, must be handled and stored securely, so as to minimise the risk of loss or theft. It must be held so as to be inaccessible to persons without the required level of security clearance (where applicable). This requirement to store such material securely applies to all those who are responsible for the handling of the material.

9.21 In particular, each public authority must apply the following protective security measures:

- physical security to protect any premises where the information may be stored or accessed;
- IT security to minimise the risk of unauthorised access to IT systems;

- an appropriate security clearance regime for personnel which is designed to provide assurance that those who have access to this material are reliable and trustworthy.

Destruction

9.22 Information obtained through covert surveillance or property interference, and all copies, extracts and summaries which contain such material, should be scheduled for deletion or destruction and securely destroyed as soon as they are no longer needed for the authorised purpose(s) set out in 9.5 above. If such information is retained, it should be reviewed at appropriate intervals to confirm that the justification for its retention is still valid. In this context, destroying material means taking such steps as might be necessary to make access to the data impossible.

Appendix 7
Covert Human Intelligence Sources Code of Practice (Sections 9.4, 9.18 – 9.25 – Dissemination, Copying, Storing and Destruction of Materials)

9.4 Dissemination, copying and retention of material obtained through a CHIS authorisation must be limited to the minimum necessary for the authorised purposes. Dissemination, copying or retention of material is necessary for the authorised purposes if:

- the material is, or is likely to become, necessary for any of the statutory purposes set out in the 2000 Act in relation to the authorisation of a CHIS;
- it is necessary to do so for facilitating the carrying out of the functions under the Act of the public authority;
- it is necessary to do so for facilitating the carrying out of any functions of the Judicial Commissioners or the Investigatory Powers Tribunal;
- it is necessary to do so for the purposes of legal proceedings; or
- it is necessary to do so for the performance of the functions of any person by or under any enactment.

Dissemination of Information

9.18 Material acquired through a CHIS authorisation may need to be disseminated both within and between public authorities, as well as to consumers of intelligence (which includes oversight bodies and the Secretary of State, for example), where necessary in order for action to be taken on it. Material which tends to indicate the presence, activity or identity of a specific CHIS should be classified and handled as highly sensitive material. The number of persons to whom such material is disclosed, and the extent of disclosure, is limited to the minimum that is necessary for one or more of the authorised purposes set out at paragraph 9.4 above. This obligation applies equally to disclosure to additional persons within a public authority and to disclosure outside the authority.

9.19 This obligation is enforced by prohibiting disclosure to persons who have not been appropriately vetted and also by the need-to-know principle in accordance with subsection (4A)(e) and

subsection (5)(e) of Section 29 of the 2000 Act: material must not be disclosed to any person unless that person's duties, which must relate to one of the authorised purposes, are such that he or she needs to know about the material to carry out those duties. In the same way, only so much of the material may be disclosed as the recipient needs. For example, if a summary of the material will suffice, no more than that should be disclosed. See also the Prosecution Disclosure Manual.

9.20 The obligations should apply not just to the original public authority, but also to anyone to whom the material is subsequently disclosed. In some cases, this will be achieved by requiring the latter to obtain the original public authority's permission before disclosing the material further. In others, explicit safeguards should be applied to secondary recipients.

9.21 The above is not intended to affect arrangements for sharing actionable intelligence in accordance with the statutory functions and procedures of public authorities.

Copying

9.22 Material obtained through a CHIS authorisation may only be copied to the extent necessary for one or more of the authorised purposes set out at paragraph 9.4 above. Copies include not only direct copies of the whole of the material, but also extracts and summaries and any other records which contain material obtained through a CHIS authorisation.

Storage

9.23 Material obtained through a CHIS authorisation and all copies, extracts and summaries which contain such material, must be handled and stored securely, so as to minimise the risk of loss or theft. It must be held so as to be inaccessible to persons without the appropriate level of security clearance (where applicable). This requirement to store such material securely applies to all those who are responsible for the handling of the material.

9.24 In particular, each public authority must apply the following protective security measures:

- physical security to protect any premises where the information may be stored or accessed;
- IT security to minimise the risk of unauthorised access to IT systems;
- an appropriate security clearance regime for personnel which is designed to provide assurance that those who have access to this material are reliable and trustworthy.

Destruction

9.25 Material obtained through a CHIS authorisation, and all copies, extracts and summaries which contain such material, should be scheduled for deletion or destruction and securely destroyed as soon as it is no longer needed for one or more of the authorised purposes set out at paragraph 9.4 above. If such information is retained, it should be reviewed at appropriate intervals to confirm that the justification for its retention is still valid. In this context, destroying material means taking such steps as might be necessary to make access to the data impossible

Appendix 8
Extracts from Home Office Covert Human Intelligence Sources Code of Practice
(Paragraphs 2.18, 2.21, 2.24-2.27)

2.18 The word “establishes” when applied to a relationship means “set up”. It does not require, as “maintains” does, endurance over any particular period. Consequently, a relationship of seller and buyer may be deemed to exist between a shopkeeper and a customer even if only a single transaction takes place. Repetition is not always necessary to give rise to a relationship, but whether or not a relationship exists depends on all the circumstances including the length of time of the contact between seller and buyer and the nature of that contact.

Example 1: Intelligence suggests that a local shopkeeper is openly selling alcohol to underage customers, without any questions being asked. A child is engaged and trained by a public authority to make a purchase of alcohol. On the basis that the exchange between a buyer and seller will be simply transactional, it is unlikely a relationship would be formed in these circumstances, and therefore it is unlikely that the child would be considered a CHIS according to the definition in Section 26(8) of the 2000 Act. A CHIS authorisation would not therefore be appropriate. However, if the test purchaser is wearing recording equipment but is not authorised as a CHIS, consideration should be given to granting a directed surveillance authorisation if it is likely to result in the obtaining of private information.

Example 2: In similar circumstances, intelligence suggests that a shopkeeper will sell alcohol to children from a room at the back of the shop, providing they have first got to know and trust them. As a consequence, the public authority decides to deploy its operative on a number of occasions, to befriend the shopkeeper and gain their trust, in order to purchase alcohol and pass back information to the public authority on the shopkeeper’s activities. In these circumstances a relationship has been established and maintained for a covert purpose and therefore a CHIS authorisation should be obtained.

2.21 In many cases involving human sources, the source will not have established or maintained a relationship for a covert purpose. Many sources provide information that they have observed or acquired other than through a relationship. This means that the source is not a CHIS for the purposes of the 2000 Act and no CHIS authorisation is required.

Example 1: A member of the public volunteers a piece of information to a member of a public authority regarding something they have witnessed in their neighbourhood. The member of the public is not a CHIS. They are not passing information obtained as a result of a relationship which has been established or maintained for a covert purpose.

Example 2: A caller to a confidential hotline (such as Crimestoppers, the HMRC Fraud Hotline, the Anti-Terrorist Hotline, or the Security Service public telephone number) reveals that they know of criminal or terrorist activity. Even if the caller is involved in the activities on which they are reporting, the caller would not be considered a CHIS as the information is not being disclosed on the basis of a relationship which was established or maintained for that covert purpose. However, should the caller be asked to maintain their relationship with those involved and to continue to supply information (or it is otherwise envisaged that they will do so), an authorisation for the use or conduct of a CHIS may be appropriate.

2.24 Tasking a person to obtain information covertly may result in a CHIS authorisation 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 the 2000 Act, for example, a directed surveillance authorisation,

may need to be considered where the activity is likely to result in the public authority obtaining information relating to a person's private or family life.

2.25 Individuals or members of organisations (e.g. travel agents, housing associations and taxi companies) who, because of their work or role have access to personal information, may voluntarily provide information to public authorities on a repeated basis and need to be managed appropriately. Public authorities must keep such human sources under constant review to ensure that they are managed with an appropriate level of sensitivity and confidentiality, and to establish whether, at any given stage, they should be authorised as a CHIS.

2.26 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 or considering whether it would be appropriate to do so.

Example: Mr Y volunteers information to a member of a public authority about a work colleague out of civic duty. Mr Y is not a CHIS at this stage as he has not established or maintained (or been asked to establish or maintain) a relationship with his colleague for the covert purpose of obtaining or disclosing information. However, Mr Y is subsequently contacted by the public authority and is asked if he would ascertain certain specific information about his colleague. At this point, it is likely that Mr Y's relationship with his colleague is being maintained and used for the covert purpose of providing that information. A CHIS authorisation would therefore be appropriate.

2.27 It is possible that a person may become engaged in the conduct of a CHIS without a public authority inducing, asking, or assisting the person to engage in that conduct. However, a CHIS authorisation should be considered, for example, where a public authority is aware that an individual is independently maintaining a relationship (i.e. "self-tasking") in order to obtain evidence of criminal activity, and the public authority intends to make use of that material for its own investigative purposes.