NEATH PORT TALBOT COUNTY BOROUGH COUNCIL

POLICY AND RESOURCES CABINET BOARD

29 JUNE 2016

REPORT OF THE HEAD OF LEGAL SERVICES – DAVID MICHAEL

MATTER FOR DECISION

WARDS AFFECTED - ALL

REGULATION OF INVESTIGATORY POWERS ACT 2000

PURPOSE OF REPORT

1. To inform members of the number of Regulation of Investigatory Powers Act 2000 Authorisations issued by the authority for the last two municipal years.

2. To replace the Authority's existing Regulation of Investigatory Powers Act 2000 Policy and Guidance with an updated Policy and Procedures.

3. To appoint the Head of Planning and Public Protection and the Head of Financial Services as Authorising Officers and Designated Persons for the purposes of the Regulation of Investigatory Powers Act 2000.

4. To designate the Head of Planning and Public Protection as the Senior Responsible Officer for the purposes of overseeing the Acquisition of Communications Data by the Authority under the Regulation of Investigatory Powers Act 2000.

BACKGROUND

5. The Regulation of Investigatory Powers Act 2000 (hereafter referred to as RIPA) controls amongst other things surveillance activities carried out by public bodies, including local authorities. In the context of local authorities, RIPA regulates such things as

test purchasing in retail premises and benefit fraud investigations for the purposes of detecting criminal offences.

6. Put simply, the Council must observe a consent procedure considering certain human rights issues before engaging in surveillance of criminal activities. It is a tool to provide the correct balance between an individual's rights to privacy and the proper use of data and surveillance in evidence gathering.

7. The main advantages of following RIPA is that surveillance authorised under it by a duly designated Authorising Officer of the Authority shall be lawful if:-

   a) An Authorisation confers an entitlement to engage in that conduct on the person whose conduct it is, and

   b) His/her conduct is in accordance with the authorisation, and

   c) The Authorisation issued by the Authorising Officer is duly approved by an Order from a Magistrate.

8. In effect it provides a lawful authority and regulatory framework for interference by a public body with an individual's human rights and privacy.

9. During recent years however the number of authorisations for covert surveillance (i.e. Director Surveillance or Use of a Covert Human Intelligence Source) issued by the authority have substantially decreased. Members are advised that only one Directed Surveillance Authorisation and no Covert Human Intelligence Source Authorisation were issued during the 2014-15 municipal year. Furthermore, members are informed that no Authorisations were issued whatsoever during the 2015-16 municipal year.

10. In view of recent changes to guidance issued by the Office of Surveillance Commissioners and other bodies it is considered that now is an appropriate time to replace the Authority's current RIPA Policy and Guidance with a new RIPA Policy and Procedures that reflects current guidance and legislation.

11. In the case of investigations carried out by the Authority's Trading Standards Department it has been the practise that any RIPA

authorisations sought were issued by the Head of Service with managerial responsibility for Trading Standards. Until recently the Head of Service and Authorising Officer for that department was Ms. Angela Thomas Head of Business Strategy and Public Protection; however due to a change in managerial responsibilities within the Authority the Trading Standards functions are now the responsibility of Ms. Nicola Pearce the Head of Planning and Public Protection. The Authority's Head of Legal Services, who has oversight responsibilities for RIPA within the Authority, therefore considers that it would be appropriate for Ms. Pearce to be designated to act as a RIPA Authorising Officer within the Authority (thereby becoming responsible for deciding whether or not authorisations sought by her officers should be granted) in place of Ms. Thomas. Ms. Pearce will not exercise this function, however, until such time as she completes a satisfactory training course on RIPA approved by the Head of Legal Services.

12. The Head of Legal Services also considers that, due to the heavy commitments of Mr. Hywel Jenkins the Director of Finance it would be advantageous to replace him as an "Authorising Officer" for the purposes of RIPA with Mr. David Rees the Authority's Head of Financial Services. Mr. Rees will not exercise this function however until such time as he has satisfied the Head of Legal Services that he has attended a satisfactory training course on RIPA.

13. The Office of Surveillance Commissioners have indicated to local authorities that they consider that an Authority's Senior Responsible Officer should preferably not act as an Authorising Officer. Accordingly, it is proposed that Mr. David Michael will cease to act as an Authorising Officer once Mrs. Nicola Pearce has undertaken a RIPA training course.

14. In addition to regulating surveillance by local authorities RIPA also controls, amongst other things, the Acquisition and Disclosure of Communications Data (such as information about the use of telephone services by individuals but not the monitoring of the content of telephone conversations). Due to the potential risk of infringement of individuals' human rights, the Act requires such activities to be controlled by persons of appropriate rank within the organisation (known as "Designated Persons").

15. In Neath Port Talbot those officers within the Authority who are appointed as Authorising Officers for RIPA surveillance also act as Designated Persons for the purposes of acquiring Communications Data. It is therefore considered appropriate that Mrs. Nicola Pearce the Head of Planning and Public Protection and Mr. David Rees the Head of Financial Services should therefore also be designated by the Authority to act as "Designated Persons" (for the purposes of acquiring Communications Data) in place of Mrs. Angela Thomas and Mr. Hywel Jenkins respectively. Both Mrs. Pearce and Mr. Rees will not however exercise their designation until such time as they have satisfied the Head of Legal Services that they have undertaken a suitable RIPA training course.

16. The processes for the Acquisition of Communications Data have been in place in the Authority for a number of years and are audited periodically by the Interception of Communications Commissioners (hereafter referred to as "IOCCO") to ensure compliance with the provisions of RIPA and the associated Statutory Code of Practice on the Acquisition and Disclosure of Communications Data.

17. The Code of Practice on the Acquisition and Disclosure of Communications Data requires the Council as best practice to appoint a Senior Responsible Officer (SRO) for the acquisition of Communications Data under RIPA. This person is responsible for:

- The integrity of the processes in place within the authority to acquire Communications Data.

- Compliance with Chapter II of Part I of RIPA and with the Code of Practice.

- Oversight of the reporting errors to IOCCO and the identification of both the cause(s) of errors and the implementation of processes to minimise repetition of errors.

- Engagement with the IOCCO inspectors when they conduct their inspections, and

- Where necessary, overseeing the implementation of post-inspection action plans approved by the Commissioner.

18. Legislative controls require the Senior Responsible Officer to hold the office, rank or position of “Designated Person”.

19. The IOCCO inspector has previously indicated to the Authority that in view of the fact that most applications for the Acquisition of Communications Data emanate from the Trading Standards Department it was appropriate that the role of the Senior Responsible Officer should be undertaken by the Head of Service for that Department provided that he/she had been authorised to act as a “Designated Person” by the Authority.

20. In consequence of the recommendation of the IOCCO Inspector Mrs. Angela Thomas the Head of Business Strategy and Public Protection was designated as the SRO for the acquisition of communications data. However, as Mrs. Thomas no longer has responsibility for trading standards it is considered that it would be more appropriate for her role as the SRO to be transferred to Mrs. Nicola Pearce Head of Planning and Public Protection: as Mrs. Pearce is now the Head of Service with responsibility for trading standards.

CONSULTATION

21. There is no requirement under the Constitution for external consultation on this item.

RECOMMENDATIONS

22. That the new RIPA Policy and Procedures a copy of which is attached hereto as Annex 1 in place of the Authority’s current RIPA Policy and Guidance be adopted.

23. That Ms. Nicola Pearce Head of Planning and Public Protection be authorised to act as an “Authorising Officer” under RIPA for covert surveillance and as a “Designated Person” for the purposes of the Acquisition and Disclosure of Communications Data under RIPA, once she has attended a suitable RIPA training course approved by the Head of Legal Services.

24. That Ms. Nicola Pearce Head of Planning and Public Protection be appointed to act as the “Senior Responsible Officer” for the purpose of the Acquisition and Disclosure of Communications Data under RIPA in place of Ms. Angela Thomas.

25. That Mr. David Rees Head of Financial Services be designated to act as an “Authorising Officer” and “Designated Person” under RIPA for covert surveillance purposes, once he has satisfied the Head of Legal Services that he has attended a training course on RIPA.

26. That Ms. Angela Thomas and Mr. Hywel Jenkins shall hereafter cease to be designated “Authorising Officers” and “Designated Persons” under RIPA.

27. That Mr. David Michael Head of Legal Services shall cease to be designated as an “Authorising Officer” and “Designated Persons” for RIPA once Ms. Pearce has received RIPA training.

REASONS FOR PROPOSED DECISION

28. To update RIPA Policy & Procedures and Officer delegations.

IMPLEMENTATION OF DECISION

29. The decision will be implemented after the three day calling period.

APPENDICES

30. Annex 1

31. **Equality Impact Assessment** – There is no requirement for an EIA for this report.

LIST OF BACKGROUND PAPERS

31. None

OFFICER CONTACT

32. Iwan Davies
Principal Litigation Solicitor
Tel (01639) 763373
i.g.davies@npt.gov.uk

33. Paul Watkins
Corporate Solicitor
Tel (01639 763761)
p.watkins1@npt.gov.uk

ANNEX 1

NEATH PORT TALBOT COUNTY BOROUGH COUNCIL

REGULATION OF INVESTIGATORY POWERS ACT 2000

POLICY AND PROCEDURES

June 2016

CONTENTS

1. Introduction

2. Benefits of Obtaining Authorisation under RIPA

3. Directed Surveillance

4. Covert Human Intelligence Sources (CHIS)

5. Authorisation Process

6. Covert Surveillance Authorised outside RIPA

7. Confidential Material

8. Joint Operations

9. Handling & Disclosure of Product

10. Use of Surveillance Devices

11. Covert Surveillance of Social Networking Sites

12. Codes of Practice

13. Scrutiny & Tribunal

Appendix 1 List of Authorising Officers

Appendix 2 List of Home Office RIPA Forms

Appendix 3 Council Procedure for Application for Magistrates Court and Application Form

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, and Guidance and Practice notes issued by the Office of the Surveillance Commissioner (OSC) 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 one of the properly trained Authorising Officers listed in Appendix 1, and dealt with in accordance with Sections 5 or 10 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 OSC 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 Officer within the Council with strategic responsibility for RIPA issues is David Michael, 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 COVERT SURVEILLANCE UNDER THE REGULATION OF INVESTIGATORY POWERS ACT FOR THE PURPOSE OF PREVENTING OR DETECTING A CRIMINAL OFFENCE PUNISHABLE BY AT LEAST 6 MONTHS IMPRISONMENT.**

12. **THE ONLY EXCEPTION TO THE ABOVE RULE IS FOR TEST PURCHASING OPERATIONS IN RELATION TO THE SALE OF ALCOHOL OR CIGARETTES TO CHILDREN.**

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 6 month custodial sentence, 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.

7. 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.

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. 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.

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

4. When considering whether 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.

5. **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, gate-keeping officer 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

- 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.

- 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 28 days) for review of the authorisation.

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

12. The gate – keeping officer 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.**

14. If, upon initial review of the authorisation, the Authorising Officer determines that it should remain in effect, reviews must take place every 28 days 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. Whenever an authorisation is cancelled, the Authorising Officer must endorse the cancellation with his/her views as to the value of the authorised activity.

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. The gate-keeping officer 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.**

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 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. Officers are reminded of the rules relating to the retention and destruction of confidential material set out in section 7 above.

2. Authorising Officers must ensure compliance with the appropriate data protection requirements and the relevant codes of practice in the handling and storage of evidential material.

3. 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.

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

5. 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.

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.

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 SNS 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 breach covertly 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.

SECTION 12 - CODES OF PRACTICE

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

2. Whilst these codes do not have the force of law, they represent best practice, 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 Office of the Surveillance Commissioner has also published useful guidance, copies of which can be obtained from his website or the gate-keeping officer.

SECTION 13 - SCRUNTINY 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 Policy and Resources Cabinet Board, who will also receive regular reports as to its implementation.

APPENDIX 1

LIST OF AUTHORISING OFFICERS

Name	Post
Michael Roberts	Head of Streetcare
David Rees	Head of Financial Services
Nicola Pearce	Head of Planning and Public Protection
Kevin Davies	Principal Benefits Officer
David Michael	Head of Legal Services and Monitoring Officer

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 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 obtain or disclose communications data, to use a covert human intelligence source or to conduct directed surveillance. Regulation of Investigatory Powers Act 2000 sections 23A, 23B, 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)

Communications Data ☐

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 obtain or disclose communications data, to use a covert human intelligence source or to conduct directed surveillance. Regulation of Investigatory Powers Act 2000 sections 23A, 23B, 32A, 32B.

Magistrates' court: West Glamorgan 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