Document Pack

Cyngor Sir Gâr
Carmarthenshire
County Council

sirgar.llyw.cymru
carmarthenshire.gov.wales

TUESDAY, 19 JANUARY 2021

TO: THE EXECUTIVE BOARD MEMBER FOR PUBLIC PROTECTION

I HEREBY SUMMON YOU TO ATTEND A VIRTUAL MEETING OF THE **EXECUTIVE BOARD MEMBER DECISIONS MEETING FOR PUBLIC PROTECTION** WHICH WILL BE HELD AT **2.00 PM,** ON **THURSDAY, 28TH JANUARY, 2021** FOR THE TRANSACTION OF THE BUSINESS OUTLINED ON THE ATTACHED AGENDA.

Wendy Walters

CHIEF EXECUTIVE

PLEASE RECYCLE

Democratic Officer:	**Kevin Thomas**
Telephone (direct line):	**01267 224027**
E-Mail:	**kjthomas@carmarthenshire.gov.uk**

Wendy Walters Prif Weithredwr, *Chief Executive,*
Neuadd y Sir, Caerfyrddin. SA31 1JP
County Hall, Carmarthen. SA31 1JP

A G E N D A

1. **DECLARATIONS OF INTEREST**
2. **DECISIONS RECORD 17TH JANUARY 2020** 3 - 4
3. **REGULATION OF INVESTIGATORY POWERS ACT** 5 - 38

Note:- The press and public are not entitled to attend the meeting. The decision record will be published normally within 3 working days.

EXECUTIVE BOARD MEMBER DECISIONS MEETING FOR PUBLIC PROTECTION

FRIDAY, 17 January 2020

PRESENT: Councillor: P.M. Hughes (Executive Board Member).

The following officers were in attendance:
R. Edgecombe, Legal Services Manager
M.S. Davies, Democratic Services Officer

Democratic Services Committee Room, County Hall, Carmarthen:10.00 am - 10.40 am

1. DECLARATIONS OF INTEREST

There were no declarations of personal interest.

2. DECISION RECORD - 26TH JULY, 2019

RESOLVED that the decision record of the meeting held on 26th July, 2019 be signed as a correct record.

3. REGULATION OF INVESTIGATORY POWERS ACT

The Executive Board Member considered a report which provided an overview of the use of covert surveillance activity undertaken by the Authority in 2019 along with the written procedures for the conduct of covert surveillance by staff and for the use of such surveillance.

The report included information in relation to the following:

- Directed Surveillance;
- Covert human Intelligence Sources;
- Interception of Communications Data;
- Unauthorised Covert Surveillance;
- Statistical Returns;
- Investigatory Powers Commissioner (IPC) Inspection.

The Executive Board Member noted that no authorisations had been issued under this Act during 2019 for the conduct of directed surveillance, covert human intelligence sources and interception of communications data.

RESOLVED that:

3.1 the covert surveillance activity undertaken by the authority in 2019 be noted;
3.2 the amendments to the corporate procedure on the conduct of such surveillance be approved for 2020.

_____ _____

EXECUTIVE BOARD MEMBER **DATE**

This page is intentionally left blank

EXECUTIVE BOARD MEMBER DECISIONS MEETING FOR PUBLIC PROTECTION

28/01/2021

Executive Board Member:	Portfolio:
Cllr. PHILIP HUGHES	PUBLIC PROTECTION

REGULATION OF INVESTIGATORY POWERS ACT

RECOMMENDATIONS / KEY DECISIONS REQUIRED:

1. **To review the covert surveillance activity undertaken by the authority in 2020**

2. **To review the corporate procedure on the conduct of such surveillance and approve changes for 2021.**

REASONS:

Guidance recommends elected members maintain an overview of the use of covert surveillance by the authority and annually review the policy and procedures governing those activities

Directorate	Designation	Tel No.
CHIEF EXECUTIVES		01267 224012
Name of Head of Service	HEAD OF ADMINISTRATION & LAW	E Mail Address:
LINDA REES JONES		LRJones@carmarthenshire.gov.uk

Declaration of Personal Interest (if any):

None

Dispensation Granted to Make Decision (if any):

N/A

(If the answer is yes exact details are to be provided below:)

DECISION MADE:

Signed:

_____

EXECUTIVE BOARD MEMBER

Recommendation of Officer adopted	YES / NO
Recommendation of the Officer was adopted **subject to the amendment(s) and reason(s) specified:**	
Reason(s) why the Officer's recommendation was **not adopted**:	

EXECUTIVE SUMMARY
EXECUTIVE BOARD MEMBER DECISION MEETING FOR PUBLIC PROTECTION

28/01/2021

REGULATION OF INVESTIGATORY POWERS ACT

Directed Surveillance

During 2020 no authorisations have been issued under this Act for the conduct of directed surveillance

Covert human Intelligence Sources

No authorisations have been issued for the use of Covert Human Intelligence Sources during 2020.

Interception of Communications Data

No applications have been made by the authority for the interception of communications data during 2020

Unauthorised Covert Surveillance
There have been no reports of unauthorised surveillance during 2020

Statistical Returns

Annual returns reflecting the above have been provided to the Office of the Surveillance Commissioner and the Interception of Communications Commissioner when requested

Covert Surveillance Procedure Document

The Councils procedure document has been reviewed and changes made to the section relating to interception of communications data to reflect changes to the application process.

DETAILED REPORT ATTACHED ?	**YES**

IMPLICATIONS

I confirm that other than those implications which have been agreed with the appropriate Directors / Heads of Service and are referred to in detail below, there are no other implications associated with this report :

Signed: **Linda Rees-Jones** **Head of Administration and Law**

Policy and Crime & Disorder	Legal	Finance	ICT	Risk Management Issues	Organisational Development	Physical Assets
NONE	**NONE**	**NONE**	**NONE**	**NONE**	**NONE**	**NONE**

CONSULTATIONS

I confirm that the appropriate consultations have taken in place and the outcomes are as detailed below

Signed: **Linda Rees Jones** **Head of Administration & Law**

(Please specify the outcomes of consultations undertaken where they arise against the following headings)

1.Local Member(s)

Not applicable

2.Community / Town Council

Not applicable

3.Relevant Partners

Not applicable

4.Staff Side Representatives and other Organisations

Not applicable

Section 100D Local Government Act, 1972 – Access to Information
List of Background Papers used in the preparation of this report:

NONE

Title of Document	File Ref No.	Locations that the papers are available for public inspection
Legal file	LS-0134	County Hall Carmarthen

COVERT SURVEILLANCE

COUNCIL PROCEDURES

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.

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.

4. Regard has been had to the Codes of Practice issued by the Home Office, and Guidance and Practice notes issued by the Office of the Surveillance Commissioner (OSC) in preparing these procedures.

5. All 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 unless the activity has been lawfully authorised under another statutory provision and the Council's Monitoring Officer has confirmed that no authorisation is therefore required in accordance with this procedure 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. **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 covert surveillance issues is Linda Rees-Jones, Head of Administration & Law

9. The 'Gate-keeping' Officer, with responsibility for vetting all covert surveillance applications and maintaining the Central Register is Robert Edgecombe, Legal Services Manager.

10. The elected member responsible for reviewing the authority's use of covert surveillance is Councillor Phillip Hughes.

SECTION 2 - BENEFITS OF OBTAINING AUTHORISATION UNDER RIPA

1. 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.

2. Furthermore, unauthorised covert surveillance activity is more likely to result in a breach of an individual's human rights, leading to a 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. Directed Surveillance occurs if it is undertaken;

- For the purposes of a specific investigation or operation

- 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

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

4. Surveillance is 'covert' if it is carried out in a manner calculated to ensure that the target is unaware it is or may be taking place. Therefore surveillance of an individual using overt CCTV cameras could still require authorisation if the cameras are targeted on that individual and he/she is unaware that they are being watched.

5. Directed surveillance becomes 'intrusive' if;

- It is carried out in relation to anything taking place on any residential premises or in any private vehicle, and

- 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/vehicle, or

- 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 vehicle, 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.

THE COUNCIL HAS NO POWER TO AUTHORISE INTRUSIVE SURVEILLANCE. IF INVESTIGATING OFFICERS HAVE ANY CONCERNS REGARDING THIS THEY SHOULD IMMEDIATELY SEEK LEGAL ADVICE.

6. 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.

7. 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 the paragraphs immediately below.

- He/she covertly uses such a relationship to obtain information or provide access to any information to another person, or
- 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 relevant Home Office Code of Practice 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.

ONLY THE CHIEF EXECUTIVE MAY AUTHORISE THE USE OF A JUVENILE CHIS.

IT IS THE POLICY OF THIS AUTHORITY TO DISCOURAGE THE USE OF COVERT HUAN INTELLIGENCE SOURCES. THE AUTHORITY WILL ONLY DEPART FROM THIS POLICY IN THE MOST EXECEPTIONAL OF CIRCUMSTANCES

SECTION 5 - AUTHORISATION PROCESS

1. Applications must be in writing, using the standard forms

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. The application form must set out in detail:

   (a) What information it is hoped the surveillance will obtain
   (b) Why that information is essential to the investigation
   (c) What steps have already been taken to obtain that information

   A sample application is attached to this document at Appendix 3

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

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

6. The gate-keeping officer may recommend changes to the application, or agree to it being submitted unaltered to a designated authorising officer.

7. Where an application must be authorised by the Chief Executive (ie 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.

8. In all other cases the investigating officer shall arrange to meet one of the authorising officers to discuss the application.

9. 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.

10. If an application is refused, the reasons for refusal shall be endorsed on the application

11. 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.

12. 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.

13. Where appropriate the gate – keeping officer will then arrange for an application to be made to the Magistrates Court for the judicial approval of the authorisation.

ALL OFFICERS MUST NOTE THAT AN AUTHORISATION REQUIRING JUDICIAL APPROVAL 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 the results of any review and communicate them to the gate-keeping officer for entry in the Central Register.

15. Once an authorising officer determines that an authorisation is no longer necessary it must be cancelled immediately.

16. 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.

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. ***(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. Where appropriate 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.

ALL OFFICERS MUST NOTE THAT WHERE A RENEWAL REQUIRES JUDICIAL APPROVAL IT WILL NOT TAKE EFFECT UNTIL IT HAS BEEN JUDICIALLY APPROVED.

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 - CONFIDENTIAL MATERIAL

1. Confidential material such as;
   (i) personal medical information
   (ii) spiritual information,
   (iii) confidential journalistic information
   (iv) information subject to legal privilege

This Information 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.

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 7 - 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 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 8 – COMMUNICATIONS DATA

1. Local authorities have no power to covertly intercept communications between third parties such as letters, text messages and telephone calls.

2. However, local authorities do have the power to give notice or seek authorisation to obtain certain types of postal and communications data such as who a particular telephone number is registered to or whether someone has asked for their mail to be diverted to another address.

3. The process for seeking such authorisations is now covered by Section 60A of the Investigatory Powers Act 2016

4. In summary, any request to access communications data must me made by the National Anti-Fraud Network (NAFN) to the Investigatory Powers Commissioners Office (IPCO) on behalf of the Council.

5. **Officers wishing to acquire communications data under this procedure should discuss their plans with the the 'Gate-Keeping' officer before approaching NAFN.**

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 the relevant section 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 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. The law 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. 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. The use of these cameras is governed by separate requirements regulated by the Surveillance Camera Commissioner.

3. Overt 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 the following rules apply;

- Where the request is made by way of an immediate response to an incident or intelligence received, no authorisation is required, subject to the requirements below.
- Where a request is made in accordance with the paragraph above and the surveillance lasts, or is likely to last for 30minutes or more, steps should be taken to obtain authorisation whilst the surveillance continues.
- Where the request is made as part of a pre-planned operation or investigation, authorisation must be obtained before any surveillance takes place.

4. 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 (ie where the 'target' is not aware that he/she is being photographed) may require authorisation.
- As a general rule, unless a covert photograph is being taken as an immediate response to an unexpected incident, authorisation should be sought.

5. 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.

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

7. 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 use of a false identity on a social networking site for this purpose is permissible, but is likely to require authorisation under the terms of this document.

3. If the monitoring of a social networking site is proposed which involves getting past access or privacy controls without the author of the site knowing that it is a public authority that is trying to gain access, then it is likely that covert surveillance is taking place which interferes with that persons human rights and authorisation will be required.

4. Any use of a Social Networking site for these purposes must also comply with Council policies on Internet and Social Media Usage.

5. ONLY THE COUNCIL'S MEDIA AND MARKETING TEAM MAY CREATE FALSE SOCIAL MEDIA PROFILES FOR USE BY COUNCIL STAFF

6. **UNDER NO CIRCUMSTANCES SHOULD COUNCIL STAFF USE THEIR PERSONAL SOCIAL MEDIA PROFILES TO CONDUCT ANY FORM OF SURVEILLANCE FOR WORK PURPOSES.**

7. For more information regarding online surveillance activity see Appendix 2

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.

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 publishes 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 review by the relevant Executive Board Member.

APPENDIX 1 – LIST OF AUTHORISING OFFICERS UNDER THE REGULATION OF INVESTIGATING POWERS ACT

Name	Post
Wendy Walters	Chief Executive
Ainsley Williams	Head of Waste
Roger Edmunds	Trading Standards Manager
Sue E Watts	Public Health Services Manager

This page is intentionally left blank

APPENDIX 2 - ONLINE COVERT ACTIVITY

(Extract from Revised code of practice on Covert Surveillance and Property Interference)

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 detail 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 is or 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 as investigative activity. This is regardless of whether a user of a website or social media platform has sought to protect such information by restricting its access by activating privacy settings.

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 activity 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.

Example 1: *A police officer undertakes a simple internet search on a name, address or telephone number to find out whether a subject of interest has an online presence. This is unlikely to need an authorisation. However, if having found an individual's social media profile or identity, it is decided to monitor it or extract information from it for retention in a record because it is relevant to an investigation or operation, authorisation should then be considered.*
Example 2: *A customs officer 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 identity, 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 of people;
- 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: *Researchers 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 analysing 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 identifiers of an individual or group are applied to the search or analysis, an authorisation should be considered.*

Below is a link to the full Code of Practice

https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/742041/201800802_CSPI_code.pdf

Below are links to the Council's Social Media and Internet Usage policies

http://intranet/media/654947/social-media-policy-2018.pdf

http://intranet/media/496059/internet-usage-and-monitoring-policy-v20.pdf

This page is intentionally left blank

APPENDIX 3 - MOCK APPLICATION

Unique Reference Number	

Part II of the Regulation of Investigatory

Powers Act 2000

Authorisation Directed Surveillance

Public Authority *(including full address)*	Carmarthenshire County Council County Hall Carmarthen, SA31 1JP		
Name of Applicant	A N Other	**Unit/Branch /Division**	Fraud Investigation Team
Full Address	County Hall Carmarthen SA31 1JP		
Contact Details	Telephone : 01267 224xxx Email: ANOther@carmarthenshire.gov.uk		
Investigation/Operation Name (if applicable)	Mr Davies		
Investigating Officer (if a person other than the applicant)			

APPENDIX 3 - MOCK APPLICATION

Unique Reference Number	

DETAILS OF APPLICATION
1 Give rank or position of authorising officer in accordance with the Regulation of Investigatory Powers (Directed Surveillance and Covert Human Intelligence Sources) Order 2010 No. 521. [1]
2 Describe the purpose of the specific operation or investigation.
The purpose of the investigation is to gather evidence of alleged offences under section 111 of the Social Security Administration Act 1992 and the Fraud Act which it is believed are being committed by Mr Davies. In particular the purpose of the proposed surveillance operation is to gather evidence to show that Mr Davies is residing with a Mrs Jones at no.82 High Street.
3 Describe in detail the surveillance operation to be authorised and expected duration, including any premises, vehicles or equipment (e.g. camera, binoculars, recorder) that may be used.
The surveillance will take the following form; 1. Direct observation by between 1 and 4 officers located in 1 or 2 unmarked vehicles parked in High Street on week day mornings 2. Surveillance will take place between 08.00 and 09.00 each day or until Mr Davies is seen leaving the property, upon which surveillance will cease. 3. The officers engaged in the surveillance will record any observations in written surveillance logs and will not make use of any cameras or other surveillance or recording devices. 4. Officers will not follow the target after he has left the premises.
4 The identities, where known, of those to be subject of the directed surveillance.
• Name: Mr A Davies • Address:82 High Street • DOB: • Other information as appropriate:
5 Explain the information that it is desired to obtain as a result of the directed surveillance.

[1] For local authorities: The exact position of the authorising officer should be given. For example, Head of Trading Standards.

Unique Reference Number	

1. Whether Mr Davies leaves the target property for work each day
2. Whether his vehicle is at the property each weekday morning

6. Identify on which grounds the directed surveillance is necessary under Section 28(3) of RIPA. ***Delete those that are inapplicable. Ensure that you know which of these grounds you are entitled to rely on (SI 2010 No.521).***

APPENDIX 3 - MOCK APPLICATION

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

7. Explain why this directed surveillance is necessary on the grounds you have identified [Code paragraph 3.3].

Information has been received from another Council department that Mr Davies is residing at the target address with Mrs Jones. If this information is correct the Mr Davies (and possibly Mrs Jones) is likely to have committed fraud in respect of a variety of applications and claims submitted to the Council, all of which have resulted in substantial sums of money being paid to Mr Davies over a number of years.

To date investigating officers have taken the following steps to obtain the required information;

(a) Searched council records for information suggesting Mr Davies lives at the target address and that Mr Davies and Mrs Jones are cohabiting
(b) Searched DVLA records which show a vehicle registered in Mr Davies's name at the target address
(c) Undertaken a credit search which shows Mr Davies has obtained credit on the basis he lives at the target address
(d) Checked marriage records, which show that Mr Davies and Mrs Jones married in 2012
(e) Mr Davies is the father of Mrs Jones daughter, born in 2014.

However this information is insufficient to prove that Mr Davies lives at the target address to the criminal standard of proof. Without further evidence that he is actually living at the property it will not be possible to progress the case further.

8. Supply details of any potential collateral intrusion and why the intrusion is unavoidable. [Bear in mind Code paragraphs 3.8 to 3.11.]

Describe precautions you will take to minimise collateral intrusion.

Unique Reference Number	

Officers conducting the surveillance will be instructed not to record anything in the surveillance logs which does not directly relate to the actions of Mr Davies. Any references to Mrs Jones and/or her daughter are to be kept to solely those which relate to their interaction with Mr Davies.

Officers should not record the activities of any other persons unless it is appropriate to do so as evidence of the commission of a crime by that person

9. Explain why this directed surveillance is proportionate to what it seeks to achieve. How intrusive might it be on the subject of surveillance or on others? And why is this intrusion outweighed by the need for surveillance in operational terms or can the evidence be obtained by any other means [Code paragraphs 3.4 to 3.7]?

Steps taken to date as outlined in box 7 above do not provide sufficient evidence to progress this investigation to conclusion. Without the additional information it is hoped to obtain by surveillance, the investigation will have to be abandoned.
The degree of intrusion into Mr Davies's family life is minimal. Only activities which can take place in full public view (i.e Mr Davies leaving the target property) will be recorded. No surveillance will take place of activities inside the property.

10. Confidential information [Code paragraphs 4.1 to 4.31].

INDICATE THE LIKELIHOOD OF ACQUIRING ANY CONFIDENTIAL INFORMATION:

NONE

APPENDIX 3 - MOCK APPLICATION

Unique Reference Number	

11. Applicant's Details			
Name (print)		**Tel No:**	
Grade/Rank		**Date**	
Signature			

12. Authorising Officer's Statement. [Spell out the "5 Ws" – Who; What; Where; When; Why and HOW– in this and the following box.]

I hereby authorise directed surveillance defined as follows: [*Why is the surveillance necessary, whom is the surveillance directed against, Where and When will it take place, What surveillance activity/equipment is sanctioned, How is it to be achieved?]*

13. Explain why you believe the directed surveillance is necessary [Code paragraph 3.3].

Explain why you believe the directed surveillance to be proportionate to what is sought to be it achieved by carrying out [Code paragraphs 3.4 to 3.7].

APPENDIX 3 - MOCK APPLICATION

Unique Reference Number	

14. (Confidential Information Authorisation.) Supply detail demonstrating compliance with Code paragraphs 4.1 to 4.31.				
Date of first review				
Programme for subsequent reviews of this authorisation: [Code paragraph 3.23]. Only complete this box if review dates after first review are known. If not or inappropriate to set additional review dates then leave blank.				
Name (Print)		**Grade / Rank**		
Signature		**Date and time**		
Expiry date and time [e.g.: authorisation granted on 1 April 2005 - expires on 30 June 2005, 23.59]				

APPENDIX 3 - MOCK APPLICATION

Unique Reference Numbe	

This page is intentionally left blank