Cyngor Sir Gâr
Carmarthenshire
County Council

sirgar.llyw.cymru
carmarthenshire.gov.wales

WEDNESDAY, 5 MARCH 2025

TO: THE CABINET MEMBER FOR ORGANISATION & WORKFORCE

I HEREBY SUMMON YOU TO ATTEND A MEETING OF THE **CABINET MEMBER FOR ORGANISATION & WORKFORCE** WHICH WILL BE HELD IN **MULTI-LOCATION - COMMITTEE ROOM 4, GROUND FLOOR, - COUNTY HALL, CARMARTHEN. SA31 1JP.**, AT **10.00 AM,** ON **WEDNESDAY, 12TH MARCH, 2025** FOR THE TRANSACTION OF THE BUSINESS OUTLINED ON THE ATTACHED AGENDA.

Wendy Walters

CHIEF EXECUTIVE

Democratic Officer:	**Emma Bryer**
Telephone (direct line):	**01267 224029**
E-Mail:	**ebryer@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 PERSONAL INTEREST**	
2.	**TO SIGN AS A CORRECT RECORD THE DECISION RECORD OF THE MEETING HELD ON THE 5TH NOVEMBER, 2024**	3 - 4
3.	**REGULATION OF INVESTIGATORY POWERS ACT**	5 - 30
4.	**PROGRESSION OF THE DEFENCE EMPLOYER RECOGNITION SCHEME (DERS)**	31 - 36

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

CABINET MEMBER FOR ORGANISATION & WORKFORCE

5 NOVEMBER 2024

PRESENT: Councillor P.M. Hughes (Cabinet Member) (In person)

The following officers were in attendance (In person):
P.R. Thomas, Assistant Chief Executive (People Management & Performance);
A. Clarke, Lead Business Partner (HR);
J. Bergiers, Lead Business Partner (H&S);
J. Owen, Democratic Services Officer.

Cabinet Member Office, County Hall, Carmarthen, SA31 1JP and remotely:
10:00am - 10:30am

1. DECLARATIONS OF PERSONAL INTEREST

There were no declarations of interest.

2. TO SIGN AS A CORRECT RECORD THE DECISION RECORD OF THE MEETING HELD ON THE 3RD MAY 2024

RESOLVED that the decision record of the meeting held on the 3rd May 2024 be signed as a correct record

3. REVISED BEHAVIOURAL STANDARDS GUIDANCE

The Cabinet Member received a report which explained that Authority's Behavioural Standards Guidance had been updated to reflect new legal duties for employers to prevent sexual harassment in the workplace.

The report highlighted that the Worker Protection (Amendment of Equality Act 2010) Act 2023 had introduced important new protections for employees, strengthening the law against sexual harassment in the workplace. The new law which came into force on 26th October 2024, placed a legal duty on the Authority to take proactive steps to prevent sexual harassment.

The Cabinet Member noted that the new law expected the Authority as an employer to take 'reasonable steps' to prevent sexual harassment. It was reported that whilst 'Reasonable steps' was not defined in the Act, and what this looked like would vary depending on the workplace. However, as a large public sector employer, the following steps would be carried out in order to strengthen the prevention of sexual harassment in the workplace:-

- Comprehensive Training
- Clear Reporting Mechanisms
- Effective Policies
- Conduct Risk Assessments
- Foster a Positive Work Culture

RESOLVED that revised Behavioural Standards Guidance be adopted.

4. HEALTH AND SAFETY POLICY

The Cabinet Member received a report which appended an amended Health and Safety Policy.

The Cabinet Member was informed that the Corporate Health and Safety Policy was a legal requirement and required a 3 yearly review. Following a recent review, minor amendments had been made to the Policy with the key changes being made to property related risk.

The Cabinet Member noted that the policy had been out for consultation across the Authority and with Trade Unions. In addition, the Corporate Health and Safety Leadership Board had approved the policy on 18th September 2024 and now sought the Cabinet Member's approval.

RESOLVED that the amended Health and Safety Policy be approved.

5. CHIEF OFFICER DISCIPLINARY PROCESS GUIDANCE

The Cabinet Member received a report on the new Chief Officer Disciplinary Process Guidance. The purpose was to create a Guidance document that would consolidate the nationally agreed disciplinary procedures that were applicable to Chief Officers outlined in the JNC Handbook, the ACAS Guidance, the Standing Orders (Wales) Regulations and the Council's Constitution, so that all relevant information was easily accessible within one document.

The Cabinet Member was informed that the Guidance document covered the Authority's Chief Executive, Directors and Heads of Service including statutory officers and should be read in conjunction with the JNC Chief Officers and Chief Executives Handbooks. The guidance document was split into 4 sections each covering the rules and procedures applicable to each group.

RESOLVED that the Chief Officer Disciplinary Process Guidance be adopted.

_____ _____

CABINET MEMBER **DATE**

12th March 2025

Cabinet Member:	Portfolio:
Cllr. Philip Hughes	Organisation and Workforce

REGULATION OF INVESTIGATORY POWERS ACT

RECOMMENDATIONS / KEY DECISIONS REQUIRED:

- To note the level of covert surveillance activity undertaken by the Council in 2024
- To approve to Councils RIPA procedures for 2025

REASONS:

- There is a requirement that elected members exercise oversight in respect of the Council's covert surveillance activity

Directorate:		Tel Nos.
Chief Executives	Designations:	01267 224018
Name of Head of Service:		
Stephen P Murphy	Head of Law Governance and Civil Services	E Mail Addresses:
Report Author:		
Robert Edgecombe	Legal Services Manager	RJEdgeco@carmarthenshire.gov.uk

Cyngor Sir Gâr
Carmarthenshire
County Council

Declaration of Personal Interest (if any): **N/A**

Dispensation Granted to Make Decision (if any): **N/A**
DECISION MADE: **Signed:** _____ DATE: _____ CABINET MEMBER

The following section will be completed by the Democratic Services Officer in attendance at the meeting

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
CABINET MEMBER DECISIONS MEETING FOR ORGANISATION AND WORKFORCE
12/03/2025

REGULATION OF INVESTIGATORY POWERS ACT

Purpose

This report gives an update on the level of covert surveillance activity by the Council and reviews the procedures that have been adopted in respect of this activity.

Background and Context

The Regulation of Investigatory Powers Act (RIPA) provides a legal framework by which the Council can seek authorisation to carry out covert surveillance in certain limited circumstances.

The Council did not authorise the conduct any covert surveillance in 2024 and indeed has not done so since 2015. There have been no reports of the Council conducting unauthorised covert surveillance during this period.

During the year the Council's Legal Services Manager received 5 queries/requests for advice in relation to Covert Surveillance. In all cases covert surveillance authorisation was unnecessary and advice was given accordingly.

Even so the Council is required to report annually regarding its use of these powers and to keep its procedures under review. There is also a need to ensure relevant staff are suitably trained and we are working with another local authority to arrange an online training session for relevant officers this year.

There have been no changes made to the attached procedure document since it was last reviewed

DETAILED REPORT ATTACHED?	**Yes**

Cyngor Sir Gâr
Carmarthenshire
County Council

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: **Steve P Murphy** **Head of Law, Goverance and Civil Services**

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

2. Legal

There is a requirement that officers report to the relevant cabinet member annually

Cyngor Sir Gâr
Carmarthenshire
County Council

CONSULTATIONS

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

Signed: Steve P. Murphy Head of Law, Goverance and Civil Services

1.Local Member(s) N/A

2.Community / Town Council N/A

3.Relevant Partners N/A

4.Staff Side Representatives and other Organisations N/A

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

Title of Document	File Ref No.	Locations that the papers are available for public inspection
Legal Depart file	**CCIP-009**	County Hall

Cyngor Sir Gâr
Carmarthenshire
County Council

This page is intentionally left blank

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, 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 and the Codes of Practice issued by the Home Office.

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 Linda Evans.

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 'fixed' CCTV cameras will not ordinarily require authorisation where their existence and use is also made clear by signage. However, where officers with responsibility for such systems are requested to allow the police (or other similar organisations) the view camera footage in real time for the purpose of targeting specific individuals, 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 the request is made as part of a pre-planned operation or investigation, the Officer with responsibility for the CCTV system in question should ask to see the RIPA authorisation (or a summary of it) 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 website.

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.

SECTION 13 - SCRUNTINY AND TRIBUNAL

The council will be subject to an inspection by an Investigatory Powers Commissioners Office (IPCO) inspector roughly every 2 years. The inspector may;

- 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 Cabinet Member.

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

Name	Post
Wendy Walters	Chief Executive
Ainsley Williams	Director of Environment
Jonathan Morgan	Head of Communities

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

12.03.25

Cabinet Member:	Portfolio:
Cllr. Philip Hughes	Organisation and Workforce

Progression of the Defence Employer Recognition Scheme (DERS)

Purpose:

To further strengthen our ongoing commitment to the Armed Forces Community and uphold our pledges to the Armed Forces Covenant.

Recommendations / key decisions required:

1. To agree '10 days additional paid leave' for HM Reserve Forces annual commitment as required for Gold Award Level. This is essential criteria.
2. To approve decision to apply for the (DERS) at Gold Award Level.
3. To agree '10 days additional paid leave' for Cadet Forces Adult Volunteers annual commitment. This is non-essential criteria.

Reasons:

To support our current and future Armed Forces Community as employees of Carmarthenshire County Council.

Directorate:	Designations:	E Mail Addresses:
Chief Executive		
Name of Head of Service: Paul Thomas	Assistant Chief Executive (People, Digital & Policy)	PRThomas@carmarthenshire.gov.uk
		GAyers@Carmarthenshire.gov.uk
Report Author: Gwyneth Ayers & Robert Young	Policy, Performance and Partnership Manager	RMYoung@carmarthenshire.gov.uk
	Lead HR Business Partner	

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: _____DATE:_____

CABINET MEMBER

The following section will be completed by the Democratic Services Officer in attendance at the meeting

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
Progression of the Defence Employer Recognition Scheme (DERS)

In October 2021 Carmarthenshire County Council (CCC) received Cabinet approval to re-sign the Armed Forces (AF) Covenant and pledge to commit to the Defence Employer Recognition Scheme (DERS). The DERS encourages employers to support serving personnel (reservists), armed forces veterans and their dependants. It aligns with the AF Covenant's pledge of respect and fairness for the AF community in the United Kingdom. CCC achieved Bronze status in February 2022 and re-affirmed its commitment to the AF community by re-signing the AF Covenant in July 2022.

In April 2023 the Cabinet approved the application for the DERS Silver Award and to work towards offering a Guaranteed Interview Scheme (GIS) for prospective employees who members of the AF community.

The Council was awarded the DERS Silver Award by the Ministry of Defence (MOD) in September 2023 and the GIS was offered in April 2024 to coincide with the rollout of the new corporate recruitment platform, which is now complete. The GIS enables us to identify, track and access this talent pool which provides a significant step towards becoming an employer of choice for the AF Community.

The DERS Gold Award is the highest recognition for employers who demonstrate outstanding support for the AF community. Securing the Gold Award would affirm CCC's commitment to supporting the AF community, enhance the Council's reputation as an inclusive and supportive employer, and broaden its access to the highly skilled AF talent pool.

To be eligible to apply for the GOLD Award CCC must meet essential criteria including providing 10 days fully paid leave for members of HM Reserve Forces to undertake their annual training commitments and duties. GOLD criteria also asks employers to consider provision of additional leave (paid) for Cadet Forces Adult Volunteers (CFAV) for them to complete their annual training commitments. The criteria in terms of CFAV is not essential for GOLD Award status.

Based on analysis undertaken of requests for unpaid leave over the last year, one employee has been identified as a reservist with no employees having been identified as serving as CFAV. On this basis it is thought that the cost of granting paid leave to both categories would be minimal.

In most cases CCC already satisfy the set criteria for GOLD (see table below) with most of the preparation work being the curating of the evidence and reviewing existing policies.

DERS ESSENTIAL GOLD CRITERIA

Gold Criteria	Council Status
Organisations must have signed the AFC	Complies
The employer must already be at Silver	Complies
The employer must have an existing relationship with RFCA Regional Employment Director	Complies
The employer must proactively demonstrate their Forces-friendly credentials as part of their	Complies

recruiting and selection processes. Where possible, they should be engaged with CTP in the recruitment of Service leavers.	Guaranteed Interview Scheme offered from April 24.
The employer must actively ensure that their workforce is aware of their positive policies towards Defence People issues. For example, an employer nominated for support to the Reserves must have an internally publicised and positive HR policy on Reserves. In the case where no HR policy exists this should be demonstrated by specific references in job descriptions or on the organisation's website	Complies. Positive people policies in place. Ongoing work to review.
The employer must be an exemplar within their market sector, advocating support to Defence People issues to partner organisations, suppliers and customers with tangible positive results. For example, demonstrate proactive steps/activity and clear success in encouraging partner organisations and their supply chain to sign the AFC	Complies
Within the context of Reserves the employer must have demonstrated support to mobilisations or have a framework in place.	Complies
The employer must demonstrate support to training by providing at least 10 days' additional paid leave for HM Reservists and CFAV.	Currently uncompliant. The Council's Time Off Policy states "*Attendance for training in the non-regular armed forces should be taken out of annual leave, flexi-leave or an application should be made for unpaid leave. All leave requests will be considered subject to service requirements*".
The employer must not have been the subject of any negative PR or media activity that could cause embarrassment to Defence.	Complies to date.

To be eligible to apply for GOLD status, CCC must approve the '10 days additional paid leave' for HM Reservists and additional leave for CFAV.

DETAILED REPORT ATTACHED?	**NO**

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: Paul Thomas, Assistant Chief Executive (People, Digital & Policy)**							
Policy, Crime & Disorder and Equalities **NONE**	Legal **NONE**	Finance **NONE**	ICT **NONE**	Risk Management Issues **NONE**	Staffing Implications **YES**	Physical Assets **NONE**	Biodiversity **NONE**

7. Staffing Implications

It should be noted that paid leave for volunteering for Armed Forces reserve training is not currently Council policy.

If it is decided to allow 10 days paid leave to reservists for their annual training commitments, this will necessitate a change to the existing Time Off Policy which states: "*Attendance for training in the non-regular armed forces should be taken out of annual leave, flexi-leave or an application should be made for unpaid leave. All leave requests will be considered subject to service requirements*"

CONSULTATIONS

I confirm that the appropriate consultations have taken in place and the outcomes are as detailed below **Signed: Paul Thomas, Assistant Chief Executive (People, Digital & Policy)**	
(Please specify the outcomes of consultations undertaken where they arise against the following headings) **1. Scrutiny Committee** N/A **2.Local Member(s)** **Name(s) of local member(s) and individual comments to be included, if appropriate.** N/A **3.Community / Town Council** **Name(s) of Town/Community Councils(s) and individual comments to be included, if appropriate** N/A **4.Relevant Partners** **Name(s) and individual comments to be included, if appropriate** N/A **5.Staff Side Representatives and other Organisations** **Name(s) and individual comments to be included, if appropriate** N/A	
CABINET MEMBER PORTFOLIO HOLDER(S) AWARE/CONSULTED YES	**Cllr. Philip Hughes has been briefed on this proposal**

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

THESE ARE DETAILED BELOW

Title of Document	File Ref No.	Locations that the papers are available for public inspection
Defence Employer Recognition Scheme		Defence Employer Recognition Scheme - GOV.UK (www.gov.uk)