PEMBROKESHIRE COUNTY COUNCIL

THE REGULATION OF INVESTIGATORY POWERS **(RIPA)** POLICY

PEMBROKESHIRE COUNTY COUNCIL

THE REGULATION OF INVESTIGATORY POWERS (RIPA) POLICY

1. INTRODUCTION

1.1 The Regulation of Investigatory Powers Act 2000 (the 2000 Act), the Investigatory Powers Act 2016 (the 2016 Act) and the Covert Surveillance and Property Interference and Covert Human Intelligence Sources Codes of Practice (the Codes), collectively referred to as RIPA, impact upon activities undertaken by the Council during the discharge of Council functions when Article 8 of the Human Rights Act 1998 - The Right to a Private Life, might be engaged covertly. This might typically be where officers undertake covert surveillance as part of their enforcement duties. The legislation and associated codes of practice in relation to RIPA provide a legal framework, with oversight of such activity internally within Pembrokeshire County Council (the Council) by virtue of the required policy, procedures and roles; and externally via the Investigatory Powers Commissioner's Office (IPCO). Those Council officers who seek to conduct such activity must first obtain authorisation from an authorising officer named within this policy. The process of application and authorisation ensures that any interference with the right to respect for private and family life as set out in the Human Rights Act 1998, is lawful, necessary and proportionate. Also, that it is conducted in accordance and within the law referred to above. Examples of enforcement functions that may require covert surveillance include trading standards, licensing, environmental and animal health enforcement. In the Council, officers in animal health enforcement and trading standards use RIPA more than any other service. Judicial oversight, by way of approval of a Justice of the Peace, is required for RIPA authorisations. RIPA authorisation is required for covert surveillance involving a specific investigation likely to result in obtaining private information (otherwise than by way of an immediate response to events) for the prevention or detection of crime involving a criminal offence which is punishable by a term of 6 months imprisonment or more; or for age-related sale of alcohol and tobacco or nicotine inhaling offences.

1.2 The Council is fully committed to complying with the Human Rights Act and

RIPA.

1.3 This Policy sets out the Council's approach to covert surveillance activities and the use of covert human intelligence sources (CHIS) falling within the RIPA framework, in order to ensure consistency, balance and fairness. It also makes it clear to the public that checks and balances apply to the Council's use of RIPA.

1.4 IPCO has responsibility for oversight of compliance with RIPA by the Council and reports directly to the government in relation to nationwide use of RIPA. In order to fulfill this function, inspectors from IPCO conduct regular inspections of the Council.

1.5 An annual report regarding the use or lack of use of RIPA powers within the Council will be made to the Elected Members of the Cabinet of the Council.

2 DEFINITION OF KEY TERMS

2.1 In order to understand the way that RIPA works, it is essential to understand the terms used in relation to RIPA, whether a particular proposed activity falls within the scope of RIPA and if any authorisation needs to be obtained, and if so, at what level.

2.2 **"Covert Surveillance"** - RIPA is only concerned with surveillance when it takes place covertly. Surveillance is covert, if and only if, it is carried out in a manner calculated to ensure that any persons who are subject to the surveillance are unaware that it is or may be taking place.

2.3 **"Intrusive Surveillance"** - Local Authorities are not permitted to carry out intrusive surveillance. Intrusive surveillance is covert surveillance that is carried out in relation to anything taking place on 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.

2.4 It should be noted that the Council is not permitted to authorise any interference with property. In any case where trespass is envisaged, officers should seek immediate advice from the Council's Senior Responsible Officer (SRO) who is Claire Incledon, Head of Legal and Democratic Services.

2.5 **"Directed Surveillance"** - Local Authorities can undertake directed surveillance. This is surveillance that is:

- covert, but not intrusive surveillance;
- conducted for the purposes of a specific investigation or operation;
- likely to result in the obtaining of private information about a person (whether or not one specifically identified for the purpose of the investigation or operation);
- conducted otherwise than by way of an immediate response to events or circumstances the nature of which is such that it would not be

reasonably practicable for an authorisation under Part II of the 2000 Act to be sought.

Directed surveillance should be necessary and proportionate to what it seeks to achieve.

2.6 **"Core functions" and "Ordinary functions"**–'core functions' are the 'specific public functions', undertaken by a particular authority, in contrast to the 'ordinary functions' which are those undertaken by all authorities (e.g. employment issues, contractual arrangements etc.)The disciplining of an employee is not a 'core function', although related criminal investigations may be.

2.7 **"Covert Human Intelligence Sources" (CHIS)** -A person is a CHIS if they establish or maintain a personal or other relationship with a person for a covert purpose, they covertly use such a relationship to obtain information or to provide access to any information; or they covertly disclose information obtained by the use of such a relationship or as a consequence of the existence of such a relationship. A CHIS could be a member of the public or a Council officer and the relationship can be the suspect or any other person. An Authorising Officer, must be satisfied that the CHIS is necessary, that the conduct authorised is proportionate to what is sought to be achieved and that arrangements for the overall management and control of the authorised activity are in force (i.e. that a handler and controller will be appointed).

2.8 **"Overt Surveillance"** - This covers all situations where surveillance is not covert. Overt surveillance does not require authorisation under RIPA because the individuals should reasonably be aware there is surveillance or monitoring being undertaken - e.g. by publicly displayed signs.

2.9 **"Surveillance"** - This includes monitoring, observing or listening to persons, their movements, their conversations or their other activities or communications. It may be conducted with or without the assistance of a surveillance device and includes the recording of any information obtained.

3 THE CODES

The Home Office website contains the Codes issued pursuant to Section 71 of the 2000 Act with the current versions of the Codes (dated August 2018) reflecting changes introduced by the 2016 Act. The Codes are also available from the Council's SRO for reference by any officer of the Council who is considering such activity, and likely to apply for, or authorise directed covert surveillance or the use of a CHIS.

4 REVIEW AND APPROVAL

This policy was reviewed and has been approved by elected members of

the Council via Cabinet. It will be placed before elected members to review on an annual basis hereafter via Cabinet and will be retained by the SRO responsible for the policy.

5 SENIOR RESPONSIBLE OFFICER (SRO)

5.1 The Council's SRO is responsible for the following matters:

- oversight and ensuring compliance with the 2000 and 2016 Acts and with the Codes;
- ensuring that processes and procedures are in place for the above and regularly checking these processes by a documented critique of areas that may engage RIPA, which is demonstrated by way of documented meeting notes retained;
- ensuring that a regular regime of dip sampling internet activity by all Council staff is carried out and documented to ensure adequate processes are in place for the use of the internet on behalf of the Council;
- pro-active oversight of applications, authorisations, and records relating to RIPA
- maintaining a central register and record of all applications, authorisations, reviews, renewals and cancellations issued or refused;
- the reporting of relevant errors to IPCO as soon as practicable and no later than 10 working days after identifying an error, with the report containing details of the cause of the error, material obtained, any untended collateral intrusion, any analysis or action taken, whether material has been destroyed or retained, a summary of steps taken to prevent recurrences and the implementation of processes to minimise repetition or errors. Examples of relevant errors include surveillance/CHIS without lawful authority or failure to adhere to safeguards within the Codes.
- ensuring authorised officers are adequately trained and of an appropriate standard
- ensuring the RIPA policy is fit for purpose
- engagement with IPCO when they conduct their inspections, where applicable
- oversight of the implementation and post-inspection action plans approved by IPCO.

5.2 Claire Incledon, Head of Legal and Democratic Services and SRO, has been responsible for overseeing the use of RIPA within the Council for a number of years and has been involved in a number of inspections of the Authority's use of RIPA.

5.3 In order to assist in the monitoring of the RIPA process within the Council, one of the Solicitors in the Legal and Democratic Services Division, Sally Martin, will have the responsibility of RIPA co-ordinator as part of her role and will be a point of contact for any Council officers requiring advice in that respect.

6 COVERT SURVEILLANCE - AUTHORISATION AND DURATION

6.1 All applications to conduct, renew or cancel directed covert surveillance or use of a CHIS must be made on one of the Council's forms used for that purpose. All such requests must be submitted to one of the designated Authorising Officers of the Council. All applications will be considered by an Authorising Officer. The Authorising Officer may, in writing, authorise the activity, refuse to authorise the activity, or authorise less of the activity requested that he/she believes is necessary and proportionate. Authorisation will only be granted by an Authorising Officer, where covert surveillance is considered to be necessary and proportionate. The power to grant, extend and cancel authorisations is limited to Authorising Officers only, in order to ensure oversight greater independence and consistency.

The authorised activity is subject to judicial approval (by a Justice of the Peace) and all authorisations and renewals granted by the Authority, will not take effect unless approved by a Justice of the Peace. Activity authorised will not be commenced until judicial approval has been obtained.

Authorisations for directed covert surveillance will cease to have effect (unless renewed or cancelled) at the end of a period of three months beginning with the time and date judicial approval has been obtained from a magistrate.

6.2 Authorising Officers are responsible for ensuring that reviews of authorisations are carried out frequently, to review compliance with that activity authorised, and the continued necessity and proportionality of the activity. An Authorisation must be cancelled as soon as it is no longer necessary and proportionate or if for some reason the activity is not being undertaken. When cancelled, the Authorising Officer must ensure that a cancellation form is completed.

6.3 **"Cancellations"** – Record the following:-

(i) Date and times that surveillance took place; and attach and retain documentation in relation to the date and time of the order to cease the activity including the date on which such instruction was given.

(ii) Date and reason for cancellation.

(iii) Confirmation that surveillance equipment has been removed.

(iv) Details of the product obtained from the surveillance and whether or not the objectives were achieved.

.

6.4 **"Emergency Situations"** - Where judicial approval of an authorisation is to be sought urgently, the authorising officer should contact Claire Incledon, SRO and Head of Legal and Democratic Services, providing all relevant information with reference to the above with the addition of a brief outline of why the matter should be heard quickly, following which liaison with the Court Clerk to arrange an urgent appointment can be carried out.

Note: - This procedure is to be used only in exceptional circumstances and a delay in internal procedure would not be deemed to be an exceptional circumstance.

6.5 All original applications and authorisations, judicial approval forms, renewals, and cancellations, together with any applications not authorised, and associated notes/documents must be submitted to Claire Incledon (SRO). These records will be indexed and retained in one central record by the SRO who is responsible for the maintenance of such records. Copies of any of this documentation can be retained within any relevant department for inclusion in investigation reports, or management purposes, however the originals must be kept within the central record. These records will be retained for 5 years.

6.6 Authorising officers for covert surveillance within the Council are:

Richard Brown
Jon Haswell
James White
Jonathan Griffiths
Darren Mutter

6.7 Particular care should be taken in cases where the subject of the investigation or operation might reasonably expect a high degree of privacy, or where confidential information is involved. Confidential information consists of communications subject to legal privilege, communications between a Member of Parliament and another person on constituency matters, confidential personal information, or confidential journalistic material. So, for example, extra care should be taken where, by undertaking surveillance of an individual it is likely that knowledge will be acquired of communications between a minister of religion and that individual relating to the latter's spiritual welfare, or between a Member of Parliament and that individual where he or she is a constituent relating to constituency matters, or wherever matters of medical or journalistic confidentiality or legal privilege may be involved. If the use of directed surveillance is likely to lead to obtaining legally privileged or confidential information then this must be authorised by the Chief Executive or in absence the person acting as Chief Executive.

7 COVERT HUMAN INTELLIGENCE SOURCES (CHIS)

7.1 As outlined above, a person is a CHIS if they establish or maintain a personal or other relationship with a person for a covert purpose, they covertly use such a relationship to obtain information or to provide access to any information; or they covertly disclose information obtained by the use of such a relationship or as a consequence of the existence of such a relationship. A CHIS could be a

member of the public or a Council officer and the relationship can be the suspect or any other person.

A relationship is used covertly, and information is disclosed covertly if the other party of the relationship is unaware of the purpose of the relationship or the disclosure of information as a result of the relationship. Actions taken by an Officer in asking or encouraging someone to act as a CHIS would also fall within the term.

An authorisation should be considered whenever the use or conduct of a CHIS is likely to engage an individual's rights under Article 8 of the European Convention on Human Rights.

A member of the public who offers information on another person voluntarily to the Council is not a CHIS. However, that person could become a CHIS if a Council Officer were to ask him/her to conduct or maintain a relationship to covertly obtain information to aid an investigation.

7.2 If the use and conduct of a CHIS is being considered, urgent advice should be sought from the Head of Legal and Democratic Services and a written application (including risk assessment) be completed recording the points outlined in the Code in that regard.

7.3 An Authorising Officer, must be satisfied that the CHIS is necessary pursuant to one of the criteria set out in the Code in that regard, that the conduct authorised is proportionate to what is sought to be achieved with reference to the elements set out in the Code in that regard and that arrangements for the overall management and control of the authorised activity are in force (i.e. that a handler and controller will be appointed) and in compliance with relevant Articles of the European Convention on Human Rights.

7.4 The Council then needs to obtain an order approving the grant or renewal of a written CHIS authorisation from a Justice of the Peace and any authorisations granted by an Authorising Officer of the Council will not take effect unless approved by a Justice of the Peace. If an authorisation is granted by an Authorising Officer of the Council, advice should also be sought from the Head of Legal and Democratic Services before making an application for judicial approval due to the risks and legal complexities involved.

7.5 Subject to certain limited exceptions, a written authorisation will, unless renewed or cancelled, cease to have effect at the end of a period of 12 months beginning with the day on which it took effect.

7.6 The Authorising Officer, who grants an authorisation will stipulate the frequency of formal regular reviews to ensure that the use or conduct of the CHIS remains within the parameters of the authorisation.

7.7 The Authorising Officer, who granted or renewed the authorisation must

cancel it if they are satisfied that the use or conduct of the CHIS no longer satisfies the criteria for authorisation or that arrangements for the CHIS' case no longer satisfy the relevant legislative requirements.

7.8 In cases where, through the use or conduct of a CHIS it is likely that knowledge of legally privileged material or other confidential information will be acquired, the deployment of the CHIS is subject to a higher level of authorisation by the Chief Executive or in absence the person acting as Chief Executive.

7.9 Confidential source records will be retained in accordance with the Regulation of Investigatory Powers (Source Records) Regulations 2000.

8 MANAGEMENT OF CHIS

8.1 A CHIS should always be allocated to a specified Council Officer as a "Handler" who will usually be of a position below that of the Authorising Officer. The Handler will have day to day responsibility for dealing with the CHIS on behalf of the Council, directing the day to day activities of the CHIS, recording the information supplied by the CHIS and monitoring the CHIS' security and welfare.

The "Controller" will normally be responsible for the management and supervision of the Handler and general oversight of the use of the CHIS.

The Controller must always complete and retain details about the use of the CHIS. The records must be readily accessible to the Handler, the SRO and IPCO.

A CHIS must never encourage another person to commit an offence.

9 CHIS- SPECIAL CONSIDERATIONS

A JUVENILES

9.1 Special safeguards also apply to the use or conduct of a juveniles, that is those under 18 years old, as sources. On no occasion should the use or conduct of a CHIS under 16 years of age be authorised to give information against their parents/any person who has parental responsibility for them. Authorisations should not be granted unless the special provisions contained within the Regulation of Investigatory Powers (Juveniles) (Order) 2000 (as amended) are satisfied. Only the Chief Executive or in absence a person acting as Chief Executive can authorise their use. The duration of such an authorisation is 4 months from the time of grant or renewal and the authorisation should be subject to at least monthly review.

The Council must ensure that an appropriate adult is present at any meetings with a CHIS under 16 years of age. The appropriate adult should normally be the parent/guardian of the CHIS unless they are unavailable or there are specific reasons for excluding them.

B VULNERABLE INDIVIDUALS

9.2 A vulnerable individual is a person who by reason of mental disorder or vulnerability, other disability, age or illness, is or may be unable to take care of themselves, or unable to protect themselves against significant harm or exploitation. Where it is known or suspected that an individual may be vulnerable, they should only be authorised to act as a CHIS in the most exceptional circumstances by the Chief Executive or in absence, the person acting as Chief Executive.

10 OBTAINING JUDICIAL APPROVAL OF AUTHORISATIONS

10.1 When making authorisations, Authorising Officers must be aware that each authorisation (or renewal of an authorisation) is subject to judicial approval.

10.2 Where an Authorising Officer has granted an authorisation for the use of directed surveillance or a CHIS, judicial approval is required. The Authority is required to make an application, without giving notice, to the Magistrates' Court. A Justice of the Peace will give approval of the grant or renewal, if at the date of the grant of the authorisation or the renewal, he/she is satisfied that the statutory tests have been met and the use is necessary and proportionate.

10.3 If the Magistrate considers that the authorisation or renewal has not met the above, approval will be refused and the authorisation can be quashed although guidance provides for 2 business days for the Council to make representations before it is quashed.

10.4 Any Authorising Officer who intends to approve an application for the use of directed surveillance or the use of a CHIS, must immediately inform the Head of Legal and Democratic Services of the details of the proposed authorisation. The Head of Legal and Democratic Services will then make the necessary arrangements for an application for an Order to approve the authorisation to be made to the Magistrates' Court.

11 ONLINE COVERT ACTIVITY

11.1 The growth of the internet, and the extent of the information that is now available online, present 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. It is important that public authorities are able to make full and lawful use of this information for their statutory purposes.

11.2 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.

When 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 and referred to elsewhere in the policy.

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 may be taking place. 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 if the intention when making such information available was not for it to be used for a covert purpose. This is regardless of whether a user has sought to protect such information by restricting access by activating privacy settings.

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.

.11.3 Any member of a public authority, or a person acting on behalf of a public authority, who intends to engage with others online or who intends to conduct activity on the internet in such a way that they may interact with others, in circumstances where the other parties could not reasonably be expected to know their true identity or without disclosing his/her identity, should consider whether the activity requires a CHIS authorisation as outlined and referred to elsewhere in the policy as a CHIS authorisation may be needed. A directed surveillance authorisation should also be considered, unless the acquisition of information is/will be covered by the terms of an applicable CHIS authorisation.

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

When engaging in conduct as a CHIS, a member of a public authority should not adopt the identity of a person known, or likely to be known, to the subject of interest or users of the site without authorisation.

12 TRAINING

It is required that training of those involved in the RIPA process be conducted

on a regular basis.

13 SURVEILLANCE EQUIPMENT

A schedule of covert surveillance equipment retained by the Council has been prepared which includes details of the team responsible for the storage, administration and use of this equipment. A copy of the schedule will be retained by the SRO and within the Public Protection Division.

14 SAFEGUARDS

Information/material obtained by means of covert surveillance or through the use or conduct of a CHIS should be handled in compliance with relevant legal frameworks as referred to in the 'Safeguards (including privileged or confidential information)' sections of the Codes.