Council of the Isles of Scilly

Surveillance procedures

Policy covering Directed Surveillance, Covert Human Intelligence Source (CHIS), Communications Data & Non-RIPA surveillance.

Updated: February 2026

Index

PART 1
COVERT SURVEILLANCE PROCEDURE (INCLUDING CHIS)

1. INTRODUCTION

1.1 In the course of carrying out its enforcement duties, the Council of the Isles of Scilly may occasionally be required to gather information via covert surveillance (for example, in the case of suspected serious criminal offences or offences relating to the underage sales of alcohol or tobacco). In doing so, we must draw a fair balance between the public interest and the rights of individuals, and we will only use the powers that are available to us when it is considered necessary and proportionate to do so.

1.2 In order to achieve that balance, the Council will comply with the Human Rights Act 1998 (HRA), the Regulation of Investigatory Powers Act 2000 (RIPA) as amended by the Protection of Freedoms Act 2012, the corresponding regulations, Procedures and Guidance issued by the Investigatory Powers Commissioners Office (IPCO) and the Codes of Practice issued by the Home Office pursuant to RIPA. The first part of the Council's Procedure sets out the Council's approach to covert surveillance issues falling within the framework of RIPA in order to ensure consistency, balance and fairness. Part 2 of the Council's Procedure deals with the acquisition and disclosure of Communications Data whilst Part 3 covers surveillance outside of the scope of RIPA. This approach will provide additional protection and safeguards where these covert activities are likely to cause us to obtain what is called 'private information' about individuals or where we go 'undercover' in certain circumstances. This Procedure also makes it clear to the public what checks and balances will apply.

1.3 The point of RIPA, to the extent that it applies to the Council, is to provide protection for the Council, individual officers and those subjected to or otherwise affected by the process. The terms of the protection are based on necessity, proportionality and the authorisation that is given in relation to a particular investigation. That said, even when RIPA is not

invoked, persons conducting activities that might interfere with the right to respect for a person's private and family life will still need to rationalise and record their reasons for not seeking authorisation under RIPA and also record how the proposed interference with that right is proportionate and necessary having regard to the HRA. If this is the case, officers should therefore consider the use of the Procedures relating to Surveillance outside of the scope of RIPA at Part 3 of this document.

1.4 The requirements set out in this Procedure are the minimum requirements which any officer, seeking to undertake surveillance using RIPA or surveillance outside of the scope of RIPA must comply with. If individual service areas wish to have additional procedures in place that is a matter for them, but they must not be to the detriment of this Procedure which ensures compliance with the legislation and related Codes of Practice.

1.5 If in any doubt about the application or relevance of any part of this Policy please seek advice from the RIPA Senior Responsible Officer (SRO) or the Monitoring Officer (detailed in Appendix A).

1.6 All persons considering the use of Directed Surveillance or a Covert Human Intelligence Source are required to have regard to this Procedure, the legislation, Procedures and Guidance issued by the Investigatory Powers Commissioner's Office and the relevant Codes of Practice. The Council's Policy can be found on the Council's website. The Codes of Practice refer to the Home Office website.

1.7 It is important that the correct forms are used and so where a Home Office form is available, that form must be used to ensure that it is the most up to date form. Home Office forms must not be stored locally or overtyped from previous applications. Either course of action may lead to avoidable errors. If in any doubt (or if you are unable to find the correct form), email surveillance@cornwall.gov.uk for further guidance.

1.8 The Council's Monitoring Officers has access to the National Anti-Fraud Network (NAFN). NAFN are appointed as the Single Point of Contact (SPoC) for obtaining Communications Data under RIPA. See Part 2 of this Policy.

While having regard to service budgets and operational necessity, you may make use of the services of NAFN for appropriate elements of this Procedure.

You must contact the Monitoring Officer in the first instance if you consider that you may need to make use of NAFN.

1.9 In addition to the Procedures set out in this document, the Council has its own Data Protection Policy that should be adhered to and read in conjunction with this Policy. The Data Protection Policy includes a paragraph relating to the investigatory use of social media platforms.

2. IMPORTANT DEFINITIONS and EXAMPLES

2.1 **'Private information'** includes any information relating to a person's private or family life, with family going beyond the formal relationship created by marriage or civil partnership. Private information is capable of including any aspect of a person's private life, or personal relationship with other, such as family, and professional business relationships. Information which is non-private may include publicly available information such as that found in newspapers, journals, on web sites, in published articles, business reports etc. This may include commercially available data where a fee may be charged, and any data which is available on request or made available at a meeting to the public.

Even though there may be a reduced expectation of privacy when in a public place covert surveillance of that person's activities will still result in obtaining private information. Surveillance of publicly accessible areas of the internet should be treated in a similar way, as there may be an expectation of privacy regarding information, in particular that on social media web sites.

Example: *two people holding a conversation on the street or on a bus may have a reasonable expectation of privacy over the contents of that conversation, even though they are associating in public. A directed surveillance authorisation would therefore be appropriate for a public authority to record or listen to the conversation as part of a specific investigation/operation.*

Private information will also include records that are reviewed to establish a pattern of behaviour, such as when different pieces of information covertly or in some cases, overtly, are used to make a permanent record about a person. Even though each individual bit of information may not be private the combined records may constitute private information.

Example: *driving past a café and taking pictures of the exterior is not likely to be regarded as directed surveillance as no private information is obtained. However, if the drive pasts were done for the purpose of establishing occupancy the data is likely to result in private information and a direct surveillance authorisation should be considered.*

Private information may also include data such as names, phone numbers, and address details. In certain circumstances the acquisition of such data may require a directed surveillance application.

Example: *It is intended to record a person giving their name and telephone number to a shop assistant in order to confirm the person's identity. Even though these details are to be disclosed in a public place there is an expectation of privacy and a directed surveillance authorisation should be considered.*

2.2 **'Confidential information'** means information subject to legal privilege, confidential personal information, confidential journalistic information and information relating to the spiritual, physical or mental health of an individual (whether living or dead) who can be identified from it, such as consultations between a health professional and a patient or information from a patient's medical records. It also includes confidential discussions between Members of Parliament. If you think that you might want to use covert surveillance to obtain such information, make sure that you seek advice first. Informal guidance from the Investigatory Powers Commissioners Office suggests that the use of covert surveillance to seek to obtain such information should be considered very carefully and can only be approved by the Chief Executive.

2.3 **'Covert Human Intelligence Source'** or **'(CHIS)'** means a person who establishes or maintains a personal or other relationship with a person for the purpose of covertly obtaining information or providing access to any information to another person or disclosing information obtained by the use of such a relationship or as a consequence of the existence of such a relationship. To be covert the relationship must be conducted in a manner that is calculated to ensure that one of the parties to the relationship is unaware of the purpose of the relationship and the use or disclosure of such information is covert if and only if one of the parties to the relationship is unaware of the use or disclosure in question. You must remember that it is the personal or other relationship between the CHIS and another person that is created or used to obtain the information

which is relevant and not the relationship between the Council Officer and the CHIS, although of course the latter must be managed correctly. It is important to note that the definition extends to CHIS activities designed to obtain any kind of information and not solely private information.

2.4 **'Use of a CHIS'** means inducing, asking or assisting a person to engage in the conduct of a CHIS or to obtain information by means of the conduct of a CHIS.

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

2.6 **'Directed Surveillance'** means surveillance which:

a) is covert but not intrusive surveillance; and
b) is undertaken for the purpose of a specific investigation or a specific operation; and
c) it is likely to result in the obtaining of private information about a person (whether or not one specifically identified for the purposes of the investigation or operation); and
d) it is conducted otherwise than by way of an immediate response to events or circumstances the nature of which are such that it would not be reasonably practicable for an authorisation to be sought for the carrying out of the surveillance. If an immediate response is appropriate in such circumstances, then the observation made would not constitute directed surveillance. This must not be abused.
e) The offence meets the Serious Crime threshold of 6 months imprisonment.

2.7 **'Intrusive Surveillance'** means covert surveillance carried out in relation to anything taking place on residential premises or in any private vehicle and that involves the presence of an individual on the premises or in the vehicle or is carried out by means of a surveillance device. This kind of surveillance may take place by means either of a person or device located inside residential premises or a private vehicle of the person who is subject to the surveillance or by means of a device placed outside which consistently provides a product of equivalent quality and detail as a product which would be obtained from a device located inside. Surveillance within the ambit of the Regulation of Investigatory Powers (Extension of Authorisation Provisions: Legal Consultations) Order 2010

(SI2010/461) is to be treated as intrusive surveillance.

Local authorities, including the Council of the Isles of Scilly, *cannot* undertake intrusive surveillance.

2.8 **'Private vehicle'** means any vehicle, including vessels, aircraft or hovercraft, which is used primarily for the private purposes of the person who owns it or of a person otherwise having the right to use it. This would include, for example, a company car owned by a leasing company and used for business and pleasure by the employee of the company.

Note: this is distinct to vehicles owned or leased by public authorities where the placing of a tracking device in the vehicle does not constitute property interference and will not be considered as covert surveillance if the staff using the vehicle are appropriately notified that such a device is in use.

2.9 **'Residential premises'** means so much of any premises as is for the time being occupied or used by any person, however temporarily, for residential purposes or otherwise as living accommodation (specifically including hotel or prison accommodation that is so occupied or used). Common areas, such as hotel dining areas or communal stairways in blocks of flats, to which a person has access in connection with their use or occupation of accommodation, are specifically excluded.

2.10 **'Collateral intrusion'** means intrusion into the lives of those not the subject of, or otherwise directly connected with the surveillance by obtaining private information about them. Where it is proposed to conduct surveillance activity specifically against individuals who are not suspected of direct or culpable involvement in the overall matter being investigated, interference with the privacy of such individuals should not be considered as collateral intrusion but as intended intrusion. Any such surveillance should be very carefully considered against the necessity and proportionality criteria.

2.11 **'Authorising Officer'** means any of the holders of the posts listed in Appendix A to this Procedure.

2.12 **'Applicant'** means a person seeking authorisation in accordance with this Procedure.

2.13 **'Covert surveillance'** means surveillance that is carried out in a manner

calculated to ensure that the person subject to the surveillance is unaware that it is or may be taking place. Note – see the section on online covert activity at 2.20 below.

2.14 **'Overt surveillance'** means surveillance that is carried out without being secretive or clandestine and which is therefore essentially open and something which the subject of the surveillance is aware of including where, for example, persons making noise are warned (preferably in writing) that if the noise continues the noise may be recorded for the purpose of the Council exercising its statutory powers or if the Council grants a licence subject to conditions saying that officers of the Council may visit without notice or without identifying themselves to check compliance with the conditions.

2.15 **'Codes of Practice'** means the Code of Practice – Covert Human Intelligence Sources and the Code of Practice – Covert Surveillance and Property Interference published by the Home Office and available on the Home Office website – www.homeoffice.gov.uk. The view has been taken that to ensure that the latest version available is considered it is appropriate to make reference to the Home Office web site rather than storing a copy locally for viewing which could lead to reliance upon an out-of-date version. Those needing to comply with the Codes of Practice may wish to store their own hard or electronic copies for ease of reference, but they should ensure from time to time that they have the latest versions. The Codes of Practice are admissible as evidence in civil and criminal proceedings and so adherence to them is critical.

2.16 **'Handler'** means the person who will conduct all day-to-day contact between a CHIS and the Council and who also has responsibility for the security and welfare of the CHIS. Usually, the Handler is a person holding a rank or position below that of the Authorising Officer.

2.17 **'Controller'** means an officer of at least the same rank as the Handler who is responsible for the management and supervision of the Handler and has general oversight of the use of the CHIS.

2.18 **'Non RIPA Surveillance'** means any Surveillance that is conducted outside of the scope of RIPA.

2.19 **'Aerial Covert Surveillance'** means surveillance using airborne crafts or devices, for example helicopters or unmanned aircraft (drones). When considering if this type of surveillance is covert particular consideration

should be given to the device used.

2.20 **'Online Covert Activity'** means the persistent study of a person's online activity or where private information about a person is obtained from any online source or private information is to be extracted and recorded from this online source this may engage privacy considerations. If online monitoring or investigating is to be conducted covertly and private information will be obtained, then an authorisation for directed surveillance should be considered.

NOTE: Where a person acting on behalf of a public authority is intending to engage with others online without disclosing their identity a CHIS authorisation may be needed.

When conducting online covert activity it should not be assumed that the there is a reduced expectation of privacy when using a social media platform. This is because the intention of the person when making the information available online was not for it to be used as part of a covert investigation. This is regardless as to whether the user of the social media site has sought to protect the information in some form or not.

When information is on sites such as Companies House there would be no reasonable expectation of privacy, posters on social media who are posting with the intent of communicating to a wide audience also can be expected to have a reduced expectation of privacy.

If a public authority conducts a reconnaissance of a site, such as a preliminary viewing to establish if the site or its contents are of interest, this is unlikely to interfere with the persons expectation of privacy and therefore is unlikely to result in a need for a directed surveillance authorisation. However, where a public authority is systematically collecting information about an individual or group, regardless of when the information was placed online, an authorisation for directed surveillance should be considered.

Example 1**:** *An officer makes an initial one-off examination of an individual's online profile to establish if they are of any relevant 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 such as identity, pattern of life, habits, intentions or associates it may be advisable to have in place an authorisation just for this single visit.*

Example 2**:** *If an officer intends to monitor a person's social media profile to extract information from it for retention because it is relevant to an investigation or operation then and authorisation should be considered.*

3. GENERAL PRINCIPLES

3.1 If there is interference by the Council with the rights of an individual under the European Convention on Human Rights and there is no lawful authority for that interference any such interference is likely to be unlawful and actionable by virtue of section 6 HRA. In addition, any evidence obtained in the absence of a lawful authorisation may, at the discretion of the Court, be excluded.

3.2 The Protection of Freedoms Act 2012 amended the 2000 Act, making RIPA authorisations subject to judicial approval. The change means that local authorities need to obtain judicial approval for the grant or renewal of an authorisation before it can take effect. In England and Wales this requires an application to be made to a Justice of the Peace. If the Justice of the Peace is satisfied that the statutory tests have been met and that the proposed surveillance is necessary and proportionate, he or she will issue an Order approving the grant or renewal for the surveillance and techniques described in the application. The amendment means that local authorities are no longer able to orally authorise the use of RIPA. All authorisations must be made in writing, approved by an Authorised Officer and then submitted to a Justice of the Peace for approval. The authorisation cannot commence until this has been done. Good Practice suggests that the Authorising Officer should be the presenting officer to the Justice of the Peace and that is the expectation of the Council under this Procedure.

3.3 A properly obtained and implemented authorisation under RIPA, including Justice of the Peace approval, will provide the Council with lawful authority to interfere with the rights of the individual. It is not simply enough that an authorisation for surveillance is obtained. It must be properly obtained, implemented, reviewed, renewed (where appropriate) and cancelled.

3.4 Failure to properly obtain and implement an authorisation under RIPA will make the surveillance unlawful and may expose the Council, and possibly the individuals concerned with the surveillance, to risk.

3.5 Even if RIPA is not engaged, because the interference with the private and family life of the subject does not amount to surveillance covered by RIPA, it will still be necessary to record in writing why the decision has been made not to seek an authorisation under RIPA. This must be done to demonstrate that the action taken has been rationalised and that the necessity and proportionality of it against the rights of the subject has been properly considered. In addition, to set out if consideration has been given to requesting whether Non-RIPA Surveillance is to be authorised – see Part 3 of these Procedures.

3.6 Obtaining authorisation for surveillance effectively suspends a person's human rights in relation to the conduct authorised and so it is essential that authorisations that are submitted to a Justice of the Peace are justifiably applied for and granted and that as soon as an authorisation is no longer needed or the surveillance has ceased the authorisation is formally cancelled.

3.7 Even though authorisations for surveillance, unless renewed or cancelled, will lapse after three months from when granted, all authorisations must be formally cancelled at the earliest appropriate opportunity using the cancellation form.

3.8 The Council **cannot** carry out intrusive surveillance.

3.9 RIPA does not deal with the material or information obtained as a result of surveillance. The managing and handling of such material of information must be strictly in accordance with the General Data Protection Regulations the Data Protection Act 2018 and the Criminal Procedure and Investigations Act 1996. Make sure you handle and manage any material properly and in accordance with these and any other statutory or other requirements that may apply from time to time. This material or information should also be handled in line with the Authorising Officer's recommendations as detailed within the approval. Failure to do so may render the material or information inadmissible as evidence as well as exposing the Council to risk.

3.10 All of the forms referred to in this procedure must be typed and signed. The copying and pasting of stock phrases is not permitted. The authorisation has to be tailor-made to suit the specific risks and circumstances of the intended surveillance operation. Make sure that you use the latest versions of the form you need by going to the appropriate

link on the Home Office website.

3.11 Some surveillance activity does not constitute intrusive or directed surveillance for the purposes of Part II of the 2000 Act and no directed or intrusive surveillance authorisation can be provided for such activity. Such activity includes:

- covert surveillance by way of an immediate response to events;
- covert surveillance as part of general observation activities;
- covert surveillance not relating to specified grounds;
- certain other specific situations;
- overt use of CCTV and Automatic Number Plate Recognition (ANPR) system.

3.12 When overt CCTV and ANPR cameras are used in a covert and pre-planned manner as part of a specific operation which is intended to conduct surveillance on a specific person or group of people, an authorisation has to be considered. Such covert surveillance is likely to result in obtaining private information about an individual and will therefore come under the definition of directed surveillance. The use of CCTV, ANPR and other overt surveillance cameras in these circumstances goes beyond their intended use for the prevention and detection of crime and the protection of the public.

3.13 All records maintained under the Act must be kept secure and confidential. A central record of all authorisations, reviews, renewals, cancellations and refusals, whatever the type of surveillance, is held on behalf of the Senior Responsible Officer and the Monitoring Officer by Cornwall Council. Copies of all such papers must be forwarded to the Monitoring Officer using the email address surveillance@cornwall.gov.uk at the earliest opportunity either by providing hard copies or scanning and providing electronic copies. If hard copies are being sent to the central record an advisory e-mail should be sent when they are sent as a check so that the officer maintaining the central record can promptly identify if any documents seem to have gone missing. Documents should be sent in sealed envelopes and marked ‘Strictly Private & Confidential’ or (preferably) delivered by hand. If being provided electronically, the original signed forms should be scanned, and they should be encrypted if appropriate. Where the Council may participate in RIPA activity under an Authorisation obtained by another agency, such as the DWP, a copy of the Authorisation must be obtained in order to ensure full understanding of what has been duly authorised prior to any Council staff participating

in the authorised activity. This copy Authorisation will be securely stored as part of the Council's central record for review or inspection as necessary, but it will be identified separately.

3.13 Save where expressly stated, the provisions of this procedure relate to both directed surveillance and the use of a CHIS.

4. SCOPE OF PROCEDURE

4.1 This Part of the Council's Procedure applies to all officers of the Council wishing to gather information by way of:

- directed surveillance; or
- the use of Covert Human Intelligence Sources.

For the purposes of convenience in this Procedure, these two areas will be collectively referred to as 'Covert Surveillance'.

4.2 Unless there is alternative legal authority, the Council's approach to Covert Surveillance is to comply with this Procedure, and therefore RIPA, and also to have regard to and comply with the Codes of Practice.

4.3 Under section 26(2)(c) of RIPA an immediate response to circumstances does not amount to directed surveillance. This must only be used when circumstances dictate and must not be abused to improperly avoid seeking authorisation when it is practicable to secure authorisation.

4.4 **It is critical that you understand that the Council can only carry out Covert Surveillance where it is necessary for the prevention or detection of crime, subject to the serious crime threshold being met or offences that relate to the underage sale of alcohol or tobacco. The serious crime threshold only applies to Directed Surveillance. Save in its capacity as Fire and Rescue Authority, the Council cannot use the protections of the RIPA application process for Covert Surveillance for any other purpose.**

4.5 To carry out Covert Surveillance authorisation must first be obtained from an Authorising Officer in accordance with this Procedure and then from a Justice of the Peace and they will not grant authorisation unless the surveillance is:

- **NECESSARY** for the purpose of preventing or detecting crime (in

accordance with the definition in the Codes of Practice, including being serious and meeting the custodial thresholds). Section 81(5) of RIPA provides that detecting crime shall be taken to include, inter alia, establishing by whom, for what purpose, by what means and generally in what circumstances any crime was committed; and

- **PROPORTIONATE** to what is sought to be achieved by carrying out the surveillance. When filling in this part of the authorisation request have regard to the prompts set out in the request which relate to:

    - why the directed surveillance is proportionate to what it seeks to achieve
    - how intrusive it might be on the subject of surveillance or on others?
    - why the intrusion is outweighed by the need for surveillance in operational terms or whether the evidence be obtained by any other means?

- In addition, measures must be taken where practicable to avoid or minimise so far as practicable Collateral Intrusion or intended intrusion.

4.6 Prior to submission to a Justice of the Peace the Authorising Officer must be certain that the following elements of balancing proportionality have been properly considered:

- balancing the size and scope of the proposed activity against the gravity and extent of the perceived crime or offence – is the proposed Covert Surveillance a “sledgehammer to crack a nut”? If it is, it is probably not proportionate. Could the intended Covert Surveillance be considered excessive or could it be less invasive?;
- explaining how and why the methods to be adopted will cause the least possible intrusion on the subject and others, whether collateral or intended;
- considering whether the activity is an appropriate use of the legislation and a reasonable way, having considered all reasonable alternatives, of obtaining the necessary result – if there are other practical ways of getting the information, they should be explored;
- evidencing, as far as reasonably practicable, what other methods have been considered and why they were not implemented – is the proposed Covert Surveillance the only practical way of getting the information needed?

The Authorising Officer ought also to consider whether the surveillance is likely to add anything to the investigation or operation and whether the resulting intelligence or evidence will significantly benefit the enquiry or chance of prosecution.

The Authorising Officer is likely to be a key witness in any challenge to the use of the RIPA procedures and so ensuring the proper consideration of all relevant issues and the recording of that consideration is fundamentally important.

4.7 Do not assume that you can simply carry out surveillance if this Procedure does not seem to apply. If in doubt get advice from the Senior Responsible Officer or the Monitoring Officer.

4.8 You are reminded that nothing in this Procedure permits the authorising or carrying out of Intrusive Surveillance.

4.9 You should also remember that surveillance is not directed surveillance if it is carried out by way of an immediate response to events or circumstances the nature of which are such that they were unforeseen and it would not be reasonably practicable for an authorisation to be sought for the carrying out of the surveillance. If an immediate response is appropriate in such circumstances, then the observation made would not constitute directed surveillance. This must not be abused. If you, for instance, leave the offices with a view to observing conduct as an immediate response to a telephone tip off then that is an immediate response to unforeseen circumstances as it would be totally impractical to obtain an Authorisation. Any surveillance carried out in this circumstance would be classed as surveillance outside of RIPA. However, it must be Human Rights Act compatible and therefore meet the test of necessity and proportionality. Conversely, if you are out of the office carrying out your duties and a completely unrelated and unforeseen set of circumstances arise then you need not obtain an authorisation before carrying out surveillance on that occasion. You must record in detail as soon as possible the circumstances, what you did and what evidence you obtained.

5. AUTHORISATIONS – DIRECTED SURVEILLANCE

5.1 Covert Surveillance within the scope of this Procedure needs to be properly authorised and recorded and at all times you are required to

ensure that the central team have oversight of your application including your risk assessment. An application for authorisation must be made in writing after first obtaining a Council of the Isles of Scilly unique reference number (URN) which is issued from the officers with responsibility for maintaining the central register. Requests for a URN should be sent to surveillance@cornwall.gov.uk and the request must include details of the proposed surveillance and the authorisation if complete at this stage. After obtaining the URN the application needs to then be authorised personally by an Authorising Officer, prior to submission to a Justice of the Peace. Applications that do not carry a centrally issued URN should not be authorised. The list of Authorising Officers (holders of the posts identified at Appendix A) may be revised in writing by the Chief Executive from time to time.

5.2 Even though those who may be authorising officers for the purposes of RIPA are prescribed in regulations (and specifically SI2010/521, as amended); the Council has decided to limit those within the authority who may authorise applications to the persons in the posts detailed in Appendix A. No other person may authorise applications. Authorising officers are not restricted to authorising or refusing applications prior to submission to a Justice of the Peace from applicants from their own service area, as it is the Council's intention that the traditional service boundaries should be broken down in this respect.

5.3 In order to commence the application process, applicants must complete and send to an Authorising Officer the standard application form available from the Home Office website, ensuring that the URN obtained from the central register team is included. Do not use locally saved versions and do not overtype previous applications as both run the risk of mistakes and unlawful authorisations.

Use the form with the name '**Directed Surveillance Application**'.

It is critically important that the extent of the covert surveillance is fully explained on the application form because the authorisation only permits the activities stated upon it. If you do not include a particular activity within the authorisation form and then conduct that activity you will not be authorised and the activity will, prima facie, be unlawful and any evidence gathered may be inadmissible.

5.4 A risk assessment will also need to be completed and this may initially be done by the Applicant. The Authorising Officer must consider the content

of the form and amend and expand upon the information provided as appropriate to ensure, so far as possible, that risk and health and safety issues are properly assessed and that review periods are stated for the assessment of risk and health and safety and that triggers for such reviews are stated as may be dictated by events or other circumstances as can be foreseen. It is a requirement of these Procedures that the risk assessment must be undertaken no more than 2 working days before the request is made for authorisation. A risk assessment form is on request from the Senior Responsible Officer or the Monitoring Officer. It is acknowledged that the operation may not start immediately on receiving the necessary authorisation from the Justice of the Peace and that in the majority of cases there will be a small gap between the authorisation being given and the authorised commencement of the surveillance operation. Consideration must always be given to reviewing the risk assessment before the surveillance operation commences where there is any delay between authorisation and commencement. Sometimes the circumstances will be such that this is not necessary and in others it will be essential. The time delay and the risks identified in the initial risk assessment will inform this decision. In any event, if there is a delay of 96 hours or more between the authorisation by the Justice of the Peace and the commencement of the surveillance the risk assessment must be reviewed. The review should be proportionate to the operation and the risks and as such need not be a particular burden. However, given that risk assessments are fundamental to the welfare of those involved in surveillance activities this important step must not be overlooked. Where a review is undertaken this must be recorded in writing. Confirmation of the review and its outcome must also be sent to surveillance@cornwall.gov.uk.

5.5 The Authorising Officer must fill in the appropriate details upon the relevant application form and the risk assessment and approve and keep a copy of those documents. This does not need to be done by the Authorising Officer within the service of the person making the request, there is an expectation that any of the Authorising Officer's named in Appendix A of this document will undertake this role. In considering the authorisation there is no requirement for the Authorising Officer to meet with the applicant as all the necessary and appropriate information should be detailed within the submitted forms. In addition, all requests for authorisation must be completed within 2 working days. Once completed a copy of the signed forms must be forwarded to the central record as above.

5.6 One of the issues to be covered in the assessment of risk for an operation or investigation, using the risk assessment form, is whether to seek public interest immunity to allow for the exclusion of material which provides the location of an observation point, in order to protect the identity of owners and occupiers of the same. Watkins LJ in R. v. Johnson [1989] 1 All ER 121 at 128, Court of Appeal, gave the following ruling for a trial judge assessing such an application [editorial in bold type]:

> "The minimum evidential requirements seem to us to be the following.
> (a) The police officer in charge of the observations to be conducted, and no one of lower rank than a sergeant **[it is suggested, in the case of the Council, the Applicant]** should usually be acceptable for this purpose, must be able to testify that beforehand he visited all observation places***** to be used and ascertained the attitude of the occupiers of premises, not only to the use to be made of them, but also to the possible disclosure thereafter of the use made and the facts which could lead to the identification of the premises thereafter and of the occupiers. He may, of course, in addition inform the court of difficulties, if any, usually encountered in the particular locality of obtaining assistance from the public.
> (b) A police officer of no lower rank than a chief inspector **[it is suggested, in the case of the Council, a Head of Service]** must be able to testify that immediately prior to the trial he visited the places used for observation, the results of which it is proposed to give in evidence, and ascertained whether the occupiers are the same as when the observations took place and, whether they are or are not, what the attitude of those occupiers is to the possible disclosure of the use previously made of the premises and of facts which could lead at trial to identification of premises and occupiers. Such evidence will of course be given in the absence of the jury **[and, it is argued, the defence]** when the application to exclude the material evidence is made".

It is for this reason that it is likely that the completed risk assessment form will be a sensitive document for disclosure purposes. Further reference should be made to the Criminal Procedure and Investigations

Act 1996 and to the Code of Practice issued pursuant to Section 23(1) of that Act.

*****Although the judgement refers to 'places' this means observation points such as a private residential address or business premises not connected to the Council.

R V Johnson does not apply to observations conducted from vehicles in a public street. The case is about the protection of person's private or business premises or about keeping the anonymity of the persons private or business premises.

5.7 Authorising Officers have the responsibility for deciding within 2 working days of receipt of the request for authorisation whether the Covert Surveillance authorisations are suitable to be authorised for submission to a Justice of the Peace and they have met all the requirements of this Procedure prior to submission. Authorisation for submission will only be given where the Authorised Officer believes that the Covert Surveillance is necessary and a proportionate response in all the circumstances and meets the statutory criteria set out in Section 28 of RIPA. Due regard must be had to the appropriate Codes of Practice and Procedures and Guidance documents.

5.8 In general, the Authorising Officer should not be directly involved in the investigation or operation in question. Should this be unavoidable for operational reasons, this should be highlighted in the information passed to the central record of authorisations.

5.9 Written authorisations will cease to have effect after three months unless renewed (by way of Authorising Officer and Justice of the Peace Approval) or cancelled (by Authorising Officer Approval). Authorisations for surveillance should be given for the appropriate length of time but in any event not longer than the maximum permitted duration of 3 months. It is considered good practice to grant authorisations for the maximum permissible period with appropriately agreed review periods. Cancellation can be at any time and so there is no detriment to anyone in granting authorisations for three months.

5.10 Authorisations for surveillance must be reviewed on a regular basis and formally cancelled when no longer needed. The review periods must be indicated in the authorisation.

5.11 All requests for authorisations must be completed in an expedient manner and it is recommended that all applications take no longer than 4 working days from the date of applying for the unique URN to submission for approval by a Justice of the Peace. Necessarily, the date of authorisation by an Authorising Officer cannot be earlier than the date of the application.

6. AUTHORISATIONS – COVERT HUMAN INTELLIGENCE SOURCES (CHIS)

6.1 The conduct and use of a CHIS within the scope of this Procedure needs to be properly authorised and recorded. An application for authorisation must be in writing to a Justice of the Peace after it has been authorised personally by an Authorising Officer. The list of Authorising Officers (holders of the posts held at Appendix A) may be revised in writing by the Chief Executive from time to time.

6.2 Even though those who may be authorising officers for the purposes of RIPA are prescribed in regulations (and specifically SI2010/521 as amended); the Council has decided to limit those within the authority who may authorise applications to the persons in the posts detailed in Appendix A - No other person may authorise applications. Authorising officers are not restricted to authorising or refusing applications prior to submission to a Justice of the Peace from applicants from their own service area as it is the Council's intention that the traditional service boundaries should be broken down in this respect.

6.3 If a CHIS is to be used as the means of Covert Surveillance, there must also be:

- a Handler (Cover Officer) of the CHIS, with day-to-day responsibility for dealing with the CHIS and for the security and welfare of the CHIS and will usually be of a rank or position below that of the Authorising Officer;
- a Controller (Covert Operations Manager) of at least the same rank as the Handler who responsibility for the management and supervision of the Handler and general oversight of the use of the CHIS. This person will usually be the Authorising Officer but if not it will be a person appointed by the Authorising Officer; and
- someone of at least the same rank as the Handler and the Controller who shall maintain records of the use made of the source but this last function could be undertaken by the Controller.

6.4 The RIPA Source Records Regulations (SI2000/2725) specify the matters/particulars of which must be included in the records relating to each CHIS. However, if you need it, make sure that you seek advice from the Monitoring Officer as to the current status of the regulations and any revised requirements there may be if you are intending to use a CHIS. The current record requirements are:

- the identity of the source;
- the identity, where known, used by the source;
- any relevant investigating authority other than the authority maintaining the records;
- the means by which the source is referred to within each relevant investigating authority;
- any other significant information connected with the security and welfare of the source;
- any confirmation made by a person granting or renewing an authorisation for the conduct or use of a source that all information has been considered and that any identified risks to the security and welfare of the source have where appropriate been properly explained to and understood by the source;
- the date when, and the circumstances in which, the source was recruited;
- the identities of the persons who, in relation to the source, are discharging or have discharged the functions mentioned in section 29(5)(a) to (c) of the 2000 Act or in any order made by the Secretary of State under section 29(2)(c);
- the periods during which those persons have discharged those responsibilities;
- the tasks given to the source and the demands made of him in relation to his activities as a source;
- all contacts or communications between the source and a person acting on behalf of any relevant investigating authority;
- the information obtained by each relevant investigating authority by the conduct or use of the source;
- any dissemination by that authority of information obtained in that way; and
- in the case of a source who is not an undercover operative, every payment, benefit or reward and every offer of a payment, benefit or reward that is made or provided by or on behalf of any relevant investigating authority in respect of the source's activities for the

benefit of that or any other relevant investigating authority.

6.5 In the case of a juvenile, or vulnerable adult CHIS the Chief Executive is the only person permitted to grant an authorisation, save that in their absence the person deputising for them may grant the authorisation.

Special safeguards apply to the use or conduct of juvenile sources (i.e. those under the age of 18). Only the Chief Executive, or in their absence, the Deputy Chief Executive can authorise the use of a juvenile as a source. On no occasion can a child under 16 years of age be authorised to give information against his or her parents or any person with parental responsibility for him or her.

6.6 An officer who wishes to use a CHIS must carry out a risk assessment to determine:

- the risk to the safety and welfare of the CHIS of any tasking; and
- the likely consequences should the role become known to the target, those involved in the target activity or any other person

The risk assessment must be updated immediately there are any changes to the risk identified or any information comes to light that indicates that a change to the identified risk might be likely.

6.7 Applicants must first obtain a Council of the Isles of Scilly URN which is issued from the officers with responsibility for maintaining the central register. Requests for a URN should be sent to surveillance@cornwall.gov.uk. After obtaining the URN the applicant needs to then complete and submit to an Authorising Officer the standard application form available from the Home Office website. Do not use locally saved versions and do not overtype previous applications as both run the risk of mistakes and unlawful authorisations. Applications that do not carry a centrally issued URN should not be authorised.

Use the form with the name '**CHIS Application**'.

It is critically important that the extent of the use and conduct of the CHIS is fully explained on the authorising form because the authorisation only permits the activities stated upon it. If you do not include a particular activity within the authorisation form and then conduct that activity you will not be authorised and the activity will, prima facie, be unlawful.

It is very important to remember the CHIS record requirements arising from the Source Records Regulations referred to below.

6.8 If the use of a CHIS is necessary, proportionate and properly authorised, the Authorising Officer must demonstrate in his or her written comments, when authorising and prior to submission to a Justice of the Peace, their awareness of the Source Records Regulations and that due attention has been paid to them. The Authorising Officer should also ensure that the necessary personal or other relationship between the CHIS and the target is properly understood and rationalised. Further, the special rules relating to the use of a juvenile or vulnerable person as a CHIS must be shown to have been considered and properly applied.

6.9 The Authorising Officer must also consider the content of the risk assessment form and amend and expand upon the information provided as appropriate to ensure, so far as possible, that risk and health and safety issues are properly assessed. The original risk assessment must not be undertaken more than 4 working days before submission to the Authorising Officer and review periods must be stated for the assessment of risk and health and safety and that triggers for such reviews are stated as may be dictated by events or other circumstances as can be foreseen. All this must also be done prior to submission to a Justice of the Peace. A risk assessment form is available on the intranet and to ensure continuity across the Council this form should be used by all services when preparing their risk assessments for RIPA applications.

6.10 The Authorising Officer must fill in the appropriate details upon the relevant application form and the risk assessment and either approve or refuse the request for authorisation. The Authorising Officer shall keep a copy of those documents.

6.11 The consideration referred to above about whether to seek public interest immunity is equally valid here.

6.12 Authorising Officers are required to undertake the authorisation of the request within 2 working days of receipt and have the responsibility for deciding whether to authorise CHIS applications for submission to a Justice of the Peace in accordance with this Procedure. Authorisation will only be submitted where the Authorised Officer believes that the proposed use of the CHIS is necessary and a proportionate response in all the circumstances and meets the statutory criteria set out in Section 29 of RIPA. Due regard must be had to the appropriate Codes of

Practice and Procedures and Guidance documents. There must be satisfactory arrangements for managing the source as required by Section 29(5) of RIPA.

6.13 It is very important that the full extent of the CHIS activities is fully explained on the authorisation form, because the authorisation only permits the activities stated upon it.

6.14 The Authorising Officer will appoint an officer to act as the designated Handler for the CHIS. The Handler will make sure that appropriate records are kept of the activities of and interaction with the CHIS. Services may devise their own forms for these purposes, though they should check with the Authorising Officer that their forms are likely to capture the correct information.

6.15 Written authorisations will cease to have effect after twelve months unless renewed or cancelled. Authorisation for the use of a juvenile source, which can only be approved by the Chief Executive, cease to have effect after one month– see currently the Regulation of Investigatory Powers (Juveniles) Order 2000/2793. Authorisations for surveillance should be given for the appropriate length of time but in any event not longer than the maximum duration.

6.16 Authorisations for surveillance must be reviewed on a regular basis and formally cancelled when no longer needed. The review periods must be indicated in the authorisation.

6.17 As one of the measures to be taken to protect the identity of the CHIS, consideration should be given to not holding the paperwork relating to the authorisation and use of the CHIS on the case file.

6.18 Each service area that wishes to use a CHIS shall appoint an administration officer who has had appropriate confidentiality training to maintain a register of every CHIS used in that service area to which access will be strictly limited according to the wishes of the Head of Service for the service area.

7. PROCEDURE FOR APPLYING FOR JUDICIAL APPROVAL

7.1 Following approval by the Authorising Officer the first stage of the process in applying for judicial approval is for the local authority to contact the administration team at the Magistrates' Court to arrange a

hearing.

7.2 The Justice of the Peace will be provided with a copy of the original RIPA authorisation setting out the case. This forms the basis of the application to the Justice of the Peace and should contain all information that is relied upon.

7.3 The original RIPA authorisation should be shown to the Justice of the Peace but will be retained by the local authority so that it is available for inspection by the Surveillance Commissioners' representative and in the event of any legal challenge or investigations by the Investigatory Powers Tribunal (IPT). The court may wish to take a copy. In addition, the Council will provide the Justice of the Peace with a partially completed judicial order form.

7.4 Although the Council is required to provide a brief summary of the circumstances of the case on the judicial application form, this is supplementary to and does not replace the need to supply the original RIPA authorisation as well.

7.5 The order will be completed by the Justice of the Peace and will be the official record of the decision of the Justice of the Peace. The Council will need to obtain judicial approval for all RIPA authorisations and renewals, and the Council will need to retain a copy of the judicial application and order after granting by the Justice of the Peace. There is no requirement for the Justice of the Peace to consider either cancellations or internal reviews.

8. REVIEWS

8.1 The Authorising Officer should determine how often the authorisation should be reviewed. This needs to be as frequently as necessary and practicable but in any event, at periods not exceeding one month both from the initial authorisation and then at regular intervals during the life of the authorisation.

8.2 The likelihood of obtaining confidential information (see section 13 below) or collateral private information relating to someone other than the subject must be borne in mind when setting the review period as proportionality will change the longer the activity continues.

8.3 If a directed surveillance authorisation provides for the surveillance of

unidentified individuals whose identity is later established the terms of the authorisation should be refined at review to include the identify of these individuals and it would be appropriate to convene a review just for this purpose. If the original authorisation considered envisages the surveillance of the individuals a fresh authorisation is not needed. If the original authorisation did not cover the direct surveillance of the individuals concerned, then a fresh authorisation is needed.

8.3 It is the responsibility of each Applicant to inform the Authorising Officer in advance of the time for a review. An authorisation monitoring form should be completed and held by the Authorising Officer and updated by the Applicant to help diarise this process.

8.4 Records of reviews will be kept as required below.

Use the form with the name **'Directed Surveillance Review'** for the review of a directed surveillance authorisation.

Use the form with the name **'CHIS Review'** for the review of a CHIS authorisation.

At all times you should keep the central team advised of the review process and forms that are used as part of the review should quote the centrally issued URN and should be sent to surveillance@cornwall.gov.uk when completed.

9. RENEWALS

9.1 As with applications for authorisation for directed surveillance, it is critical to the lawfulness of the authorisation and the resultant surveillance, and hence the admissibility of evidence, that particular attention is given to proportionality. There is a legitimate line of attack against an authorisation, the surveillance based upon it and the evidence gathered if the previously authorised surveillance has failed to gather the evidence that was sought or the proportionality of the surveillance has otherwise diminished since authorisation. If you are considering applying for a renewal you should proceed on the basis that with each application for renewal the burden of satisfying the proportionality requirement increases. It is simply not acceptable to recite what has previously been recorded as to proportionality as the circumstances will be different, surveillance having already been carried out for a period. If you are seeking to renew an application that has resulted in the obtaining of

confidential information that fact should be highlighted in the renewal application which requires approval from the Chief Executive.

Should the Renewal be challenged in Court it will be for the Applicant and Authorising Officer to justify their actions in Court.

9.2 Authorisations may be renewed by a Justice of the Peace for a further period of three months (twelve months for CHIS or one month for a juvenile CHIS) provided an Authorising Officer is satisfied, prior to submission, that the request continues to meet the criteria. The relevant standard renewal application forms must be used except in cases of urgency.

Use the form with the name **'Directed Surveillance Renewal'** for the renewal of a directed surveillance authorisation.

Use the form with the name **'CHIS Renewal'** for the renewal of a CHIS authorisation.

It is critical that when making an application for a renewal you have regard to paragraph 9.1 as to the need to pay particular attention to proportionality at each renewal and at specified reviews between renewals.

9.3 Where renewals are timetabled to fall outside of court hours, for example during a holiday period, it is the Council's responsibility to ensure that the renewal is completed ahead of the deadline. Out of hours procedures are for emergencies and should not be used because a renewal has not been processed in time.

9.4 Authorisations can be renewed more than once but note above at paragraph 9.1 the need to pay particular attention to proportionality at each renewal and at reviews between renewals.

9.5 Records of renewals will be kept as required below.

9.6 It is the responsibility of each Applicant to ensure the timely processing of a renewal application. A monitoring form should be completed and held by the Authorising Officer and updated by the Applicant to help diarise this process.

9.7 All renewals MUST carry the centrally issued URN and all application for

renewals should be sent to the central team as well as the authorising officer and, once completed, renewals should be forwarded to surveillance@cornwall.gov.uk.

10. CANCELLATIONS

10.1 It is not acceptable to proceed on the basis that an authorisation has lapsed as all authorisations are required to be formally cancelled at the earliest appropriate time. The Authorising Officer must cancel the authorisation if satisfied that the activity no longer meets the criteria upon which it was or could have been authorised or satisfactory arrangements for the use of the CHIS no longer exist. The standard cancellation forms must be used.

Use the form with the name **'Directed Surveillance Cancellation'** for the cancellation of a directed surveillance authorisation and ensure you include the URN.

Use the form with the name **'CHIS Cancellation'** for the cancellation of a CHIS authorisation and ensure you include the URN.

10.2 Authorisations must be formally cancelled upon completion of the operations to which they relate or where they are no longer necessary or proportionate. The Applicant should be identifying on the cancellation form if the surveillance objectives were met. The Authorising Officer should be providing advice on the management of the product of the surveillance as well and providing instructions with regard to the removing of any devices deployed in the surveillance activity

10.3 As soon as the decision is taken that the directed surveillance should be discontinued the instruction must be to stop all surveillance as soon as is reasonably practical.

10.4 The date the authorisation was cancelled must be centrally recorded and records of cancellation must be sent to surveillance@cornwall.gov.uk.

11. JOINT WORKING WITH OTHER AGENCIES

11.1 It may from time to time be appropriate to mount joint surveillance operations with other agencies. The tasking or lead agency should authorise the operation under its own covert surveillance procedure, subject to judicial approval. It is important to avoid duplication and to

ensure that parallel surveillance does not prejudice another operation by another body.

11.2 An example is where a police officer of at least superintendent rank requests the use of CCTV staff and equipment to monitor specific areas at specific times. The police officer, on behalf of the police as the tasking agency, should authorise the operation under the covert surveillance procedure of the police. The appropriate paperwork, and particularly the authorisation, should be sent to the Council's CCTV supervisor prior to the start of the operation. In an emergency or where this is impracticable, the completed form should be faxed to the operation centre, and the supervisor can check and query or approve the form and the use of the CCTV system retrospectively. The police authorisation may contain a request for directed and intrusive surveillance for the additional grounds not available to the Council, such as public safety.

11.3 Where the Council may operate under an Authorisation obtained by another agency a copy of the Authorisation must be obtained in order to ensure full understanding of what has been duly authorised and prior to any Council staff participating in the authorised surveillance. This copy Authorisation will be kept with the Council's central record for review or inspection as necessary, but it will be separately identified.

12. RECORDS

12.1 All surveillance activity requires a URN issued by the officers with responsibility for maintaining the central register. Authorising Officers should decline to deal with any applications for authorisation or paperwork for any of the subsequent stages unless a centrally issued URN is included.

12.2 A central register of all authorisations, reviews, renewals, cancellations and refusals under this Part of this Procedure will be held on behalf of the Monitoring Officer and all forms associated with each of the above steps in the process should be forwarded to surveillance@cornwall.gov.uk for inclusion in the register. This register must be updated whenever an authorisation is granted, reviewed, renewed, cancelled or refused. This will be achieved by the Authorising Officer forwarding the original application as approved, the review, renewal, cancellation, or refusal to surveillance@cornwall.gov.uk and all such records held centrally will be retained for at least five years.

12.3 The Applicant will retain copies of the original forms of authority, review, renewal, cancellation or refusal and in addition will hold:

- A record of the application for and receipt of the URN.
- Details of attendances at the Magistrates' Court.
- Any separate notification of approval given by the Authorising Officer.
- A copy of the order approving the grant or renewal of an Authorisation from a Justice of the Peace.
- A record of the period over which surveillance has taken place.
- The frequency of reviews conducted by the Authorising Officer in the case.
- A record of the result of each such review.
- The date and time of any instruction given by the Authorising Officer.
- Records of the use of a particular CHIS, any risk assessment in relation to the source, the value of the source, the circumstances in which tasks were given to the source and any other record required by regulation.
- A note of when and how documents have been submitted to the central register.

12.4 All records maintained under the Act must be kept secure and confidential and the measures set out in paragraph 3.13 followed when documents are being sent to the central register.

12.5 The proper keeping of records, including the central record, is also important for the quarterly reporting that is required to Members on the amount and nature of the use of RIPA that has occurred and also to allow Members to effectively consider the confirmation or variation, as appropriate and if necessary, of this Procedure on an annual basis as required by the Codes of Practice.

13. CONFIDENTIAL INFORMATION

13.1 Although RIPA does not provide any special protection for confidential information, particular consideration should be given if the directed surveillance may result in confidential information might being obtained. Further guidance is available in the relevant Codes of Practice.

13.2 Where it is likely that confidential information will be acquired activity must be authorised by the Chief Executive (or in the absence of the Chief Executive the person deputising for them). In general, legal advice

should be obtained prior to any activity that is likely to acquire confidential information.

13.3 If an investigation is going to seek information about lawyers, priests, doctors or journalists in relation to their professional activities, advice must be sought from the Monitoring Officer.

14. RECORD KEEPING AND DATA PROTECTION

14.1 All records referred to in this procedure will be retained for a period of five years from the ending of the authorisation or last renewal. These records will be kept in a secure file, with access limited to the appropriate officers.

14.2 The central register will be kept as referred to elsewhere in this Procedure and will contain the following information:

- the centrally issued URN of the investigation or operation;
- the type of authorisation;
- the date the authorisation was given;
- the review date of the authorisation;
- the name and grade of the authorising officer who approved the application for submission to the Justice of the Peace;
- the order granted by a Justice of the Peace
- the title of the investigation or operation, including a brief description and names of subjects, if known;
- whether the urgency provisions were used, and if so why;
- if the authorisation has been renewed, the renewal which will set out when it was renewed and who authorised the renewal, including the name and grade of the authorising officer who approved the renewal submission to a Justice of the Peace;
- any paperwork relating to a renewal;
- whether the investigation or operation is likely to result in obtaining confidential information as defined in this code of practice;
- whether the authorisation was granted by an individual directly involved in the investigation; and
- the date the authorisation was cancelled and the cancellation paperwork.

14.3 In relation to CHIS authorisations, these records need only contain the name, code name, or unique identifying reference of the CHIS, the date

the authorisation was granted, renewed or cancelled and an indication as to whether the activities were self-authorised.

14.4 As appropriate, the authority's data protection advisors will be consulted to ensure that material is handled, stored and disposed of in accordance with the requirements of the General Data Protection Regulations and the Data Protection Act 2018.

14.5 Records kept in relation to CHIS authorisations shall be maintained in such a way as to preserve confidentiality, prevent disclosure of the identity of the CHIS and prevent disclosure of the information provided by that CHIS.

14.6 All information that is obtained through covert surveillance and all copies, extracts and summaries (which contain such material) are subject current data protection legislation and therefore must be scheduled for deletion/destruction as soon as it is no longer needed for the purpose(s) for which it was obtained. If there is a need to retain such information the reason for its retention should be reviewed on a regular basis to ensure its continuing retention is still justified.

15. GENERAL/COMPLAINTS

15.1 This Procedure is a public document and will be available for public inspection at Old Wesleyan Chapel, Garrison Lane, St Mary's, Isles of Scilly, TR21 0JD and upon the Council's website or by emailing surveillance@cornwall.gov.uk. The procedure will be reviewed and updated from time to time by the Monitoring Officer in consultation with appropriate colleagues

15.2 Complaints concerning the way in which the Council has operated this procedure may be made to Council of the Isles of Scilly, Old Wesleyan Chapel, Garrison Lane, St Mary's, Isles of Scilly, TR21 0JD or dpo@scilly.gov.uk

15.3 The Investigatory Powers Tribunal has the jurisdiction to investigate and determine complaints on the use of investigatory powers by a public authority. Complaints about the use of these powers by the Council of the Isles of Scilly should be sent to:

The Investigatory Powers Tribunal
PO Box 332220
London
SW1H 9ZQ

PART 2
ACQUISITION & DISCLOSURE OF COMMUNICATIONS DATA POLICY & PROCEDURE

1. INTRODUCTION

1.1 In the course of carrying out its enforcement duties, the Council of the Isles of Scilly may occasionally be required to gather information via covert surveillance (for example, in the case of suspected serious criminal offences or offences relating to the underage sales of alcohol or tobacco). In doing so, we must draw a fair balance between the public interest and the rights of individuals and we will only use the powers that are available to us when it is considered necessary and proportionate to do so.

1.2 In order to achieve that balance, the Council will comply with the Human Rights Act 1998 (HRA), the Regulation of Investigatory Powers Act 2000 (RIPA) as amended by the Protection of Freedoms Act 2012, the corresponding regulations, any procedures or guidance that might be issued by the IOCCO and the Codes of Practice issued by the Home Office pursuant to RIPA. This Part of the Council's Procedure sets out the Council's approach to the acquisition of Communications Data falling within the framework of RIPA in order to ensure consistency, balance and fairness. Part I of the Council's Procedure deals with covert surveillance and the use of covert human intelligence sources. This approach will provide additional protection and safeguards where these covert activities are likely to cause us to obtain what is called 'private information' about individuals or where we go 'undercover' in certain circumstances. This Procedure also makes it clear to the public what checks and balances will apply.

1.3 The point of RIPA, to the extent that it applies to the Council, is to provide protection for the Council, individual officers and those subjected to or otherwise affected by the process. The terms of the protection are based on necessity, proportionality and the authorisation that is given in relation to a particular investigation. That said, even when RIPA is not invoked, persons conducting activities that might interfere with the right

to respect for a person's private and family life will still need to rationalise and record their reasons for not seeking authorisation under RIPA and also record how their proposed interference with that right is proportionate and necessary having regards to the HRA.

1.4 The requirements set out in this Procedure are the minimum requirements which any officer seeking to use RIPA must comply with. If individual service areas wish to have additional procedures in place that is a matter for them, but they must not be to the detriment of this Procedure which ensures compliance with the legislation and related Codes of Practice.

1.5 The Council is not permitted to intercept communications which means to monitor or modify a telecommunication system in order to make some or all of the contents of the communication available, while being transmitted, to a person other than the sender or intended recipient of the communication.

1.6 If in any doubt about the application or relevance of any part of this policy, please seek advice from the RIPA Senior Responsible Officer or the Monitoring Officer.

1.7 All persons considering the acquisition of Communications Data are required to have regard to this Procedure, the legislation, any procedures or guidance issued by the IOCCO and the relevant Codes of Practice.

1.8 It is important that the correct forms are used and so where a Home Office form is available, that form must be used to ensure that it is the most up to date form. Home Office forms must not be stored locally or overtyped from previous applications. Either course of action may lead to avoidable errors.

1.9 The Council's Monitoring Officer is subscribed to the National Anti-Fraud Network (NAFN). The NAFN web site states that NAFN:

- NAFN are appointed as the Single Point of Contact (SPoC) for obtaining Communications Data under RIPA.
- While having regard to service budgets and operational necessity, you may make use of the services of NAFN for appropriate elements of this Procedure.

1.10 In addition to the Procedures set out in this document, the Council has its

own Data Protection Policy that should be adhered to and read in conjunction with this Policy. The Data Protection Policy includes a paragraph relating to the investigatory use of social media platforms.

2. IMPORTANT DEFINITIONS

2.1 To the extent relevant to this Part of the Council's Procedure, the definitions set out in Part I of the Procedure apply equally to this Part and the use of those terms must be taken as so defined for this Part unless otherwise indicated.

2.2 **'Communications Data'** means the 'who', 'when' and 'where' of the communication but not the content, not what was said or written, but includes the manner in which, and by what method, a person or machine communicates with another person or machine and is defined within the Act.

2.3 '**Entity Data and Event data'**

Entity data
This data is about entities or links between them and describes or identifies the entity but does not include information about individual events. Entities could be individuals, groups and objects (such as mobile phones or other communications devices).

An entity can also include devices so this data would cover information about the devices owned by a customer as well as the services provided by the telecommunications operator to which the owner of the devices subscribes. This data may include names and addresses of subscribers.

Entity data covers information about a person or thing, and about links between a telecommunications service, part of a telecommunication system and a person or thing, that identify or describe the person or thing. This means that individual communication devices such as phones, tablets and computers are entities. The links between a person and their phone are therefore entity data but the fact of or information about communications between devices on a network at a specific time and for a specified duration would be events data.

Examples of entity data include:

- 'subscriber checks' such as "who is the subscriber of phone number

01234 567 890?", "who is the account holder of e-mail account example@example.co.uk?" or "who is entitled to post to web space www.example.co.uk?";

- 'subscribers' or account holders' account information, including names and addresses for installation, and billing including payment method(s), details of payments;
- information about the connection, disconnection and reconnection of services to which the subscriber or account holder is allocated or has subscribed (or may have subscribed) including conference calling, call messaging, call waiting and call barring telecommunications services;
- information about apparatus or devices used by, or made available to, the subscriber or account holder, including the manufacturer, model, serial numbers and apparatus codes; and information about selection of preferential numbers or discount calls.

Events Data

For the Council the lawful purpose for obtaining Entity Data is it must be "serious crime", defined in section 86(2A) of the Act means: an offence for which an adult is capable of being sentenced to one year or more in prison; any offence involving violence, resulting in a substantial financial gain or involving conduct by a large group of persons in pursuit of a common goal; any offence committed by a body corporate; any offence which involves the sending of a communication or a breach of privacy; or an offence which involves, as an integral part of it, or the sending of a communication or breach of a person's privacy.

Events Data is more intrusive. It identifies or describes events in relation to a telecommunication system which consist of one or more entities engaging in an activity at a specific point, or points, in time.

Events data covers information about time-bound events taking place across a telecommunication system at a time interval. Communications data is limited to communication events describing the transmission of information between two or more entities over a telecommunications service. This will include information which identifies, or appears to identify, any person, apparatus or location to or from which a communication is transmitted. It does not include non-communication events such as a change in address or telephone number for a customer.

Examples of events data include, but are not limited to:

- information tracing the origin or destination of a communication that is, or has been, in transmission (including incoming call records);
- information identifying the location of apparatus when a communication is, has been or may be made or received (such as the location of a mobile phone);
- information identifying the sender or recipient (including copy recipients) of a communication from data comprised in or attached to the communication;
- routing information identifying apparatus through which a communication is or has been transmitted (for example, file transfer logs and e-mail headers – to the extent that content of a communication, such as the subject line of an e-mail, is not disclosed);
- itemised telephone call records (numbers called);
- itemised internet connection records;
- itemised timing and duration of service usage (calls and/or connections);
- information about amounts of data downloaded and/or uploaded;
- information about the use made of services which the user is allocated or has subscribed to (or may have subscribed to) including conference calling, call messaging, call waiting and call barring telecommunications services.

UNDER NO CIRCUMSTANCES CAN THE CONTENT OF A COMMUNICATION BE OBTAINED.

2.4 **'Applicant'** is a person involved in conducting an investigation or operation for a relevant public authority who makes an application in writing or electronically for the acquisition of Communications Data. The Applicant completes an application form, setting out for consideration by the designated person, the necessity and proportionality of a specific requirement for acquiring Communications Data. Applications may be made orally in exceptional circumstances, but a record of that application must be made in writing or electronically as soon as possible.

2.5 **'Designated Person'** is a person holding prescribed office (holders of the posts held at Appendix A) in the Council who considers the application and records their considerations at the time (or as soon as reasonably practicable) in writing or electronically. If the Designated Person believes it is necessary and proportionate in the specific circumstances, the acquisition is verified for submission to NAFN and this will then be forwarded to the Office of Communications Data (OCDA)

foe authorisation. Individuals who undertake the role of a designated person must have current working knowledge of human rights principles, specifically those of necessity and proportionality and how they apply to the acquisition of Communications Data under the code of practice for the acquisition and disclosure of Communications Data. Designated Persons must ensure they only verify requests for submission to NAFN only for purposes and only in respect of types of communications data that a Designated Person of their office, rank or position in the relevant public authority may grant. The Designated Person shall assess the necessity for any conduct to acquire or obtain Communications Data taking into account any advice provided by the single point of contact (SPoC). Additionally, Designated Persons should not be responsible for granting authorisations in relation to investigations or operations in which they are directly involved. However, where this is unavoidable justification for taking the role of designated person must be explicit in their considerations.

2.6 **'Single Point of Contact' (SPoC)** is either an accredited individual or group of accredited individuals trained to facilitate lawful acquisition of Communications Data and effective co-operation between a public authority and Communications Service Providers (CSP's). An accredited SPoC promotes efficiency and good practice in ensuring only practical and lawful requirements for Communications Data are undertaken. The SPoC provides objective judgement and advice to both the applicant and designated person. In this way the SPoC provides a "guardian and gatekeeper" function ensuring that the Council acts in an informed and lawful manner. In line with Home Office Guidance Cornwall Council utilise the SPoC function offered by the National Anti-Fraud Network (NAFN).

2.7 **'Senior Responsible Officer'** is responsible for:

- *the* integrity of the process in place within the public authority to acquire communications data;
- compliance with Chapter II of Part I of the Act and with this code;
- oversight of the reporting of errors to the IOCCO and the identification of both the cause(s) of errors and the implementation of processes to minimise repetition of errors;
- engagement with the *IOCCO inspectors when they conduct their inspections, and where necessary, oversee the implementation of post-inspection action plans approved by the Commissioner.*

2.8 **'Communications Service Provider'** or **'CSP'** means an operator who provides a postal or telecommunications service.

3. GENERAL PRINCIPLES

3.1 The acquisition of Communications Data under the RIPA involves four roles within a relevant public authority before submission to a Justice of the Peace:

- **the Applicant**
- **the Designated Person**
- **the Single Point of Contact**
- **the Senior Responsible Officer**

3.2 If there is interference by the Council with the rights of an individual under the European Convention on Human Rights and there is no lawful authority for that interference any such interference is likely to be unlawful and actionable by virtue of Section 6 HRA. In addition, any evidence obtained in the absence of a lawful authorisation may, at the discretion of the Court, be excluded.

3.3 Approvals need to be initially verified by a designated officer before forwarding to NAFN. If they are satisfied and that the statutory tests have been met and that the proposed acquisition of Communications Data is necessary and proportionate, this will be forwarded to OCDA for final approval.

3.4 Properly following the procedures set out in this Part of this Procedure will provide the Council with lawful authority to interfere with the rights of the individual.

3.5 Failure to properly to follow this Procedure and to properly obtain and implement will make the obtaining of Communications Data unlawful and may expose the Council, and possibly the individuals concerned with the obtaining of the data, to risk.

3.6 Even if RIPA is not engaged, because the interference with the private and family life of the subject does not amount to activity covered by RIPA, it will still be necessary to record in writing why the decision has been made not to seek an authorisation under RIPA in order to demonstrate that the action taken has been rationalised and the necessity and proportionality of it against the rights of the subject has

been properly considered. See paragraph 1.3 as to HRA related records being made.

3.7 Obtaining approval for the acquisition of Communications Data under this Procedure effectively suspends a person's human rights in relation to the conduct authorised and so it is essential that authorisations that are submitted to a Justice of the Peace are justifiably applied for and granted and that there is no inappropriate use of the Procedure.

3.8 RIPA does not deal with the managing and handling of Communications Data obtained in accordance with this Part of this Procedure and such data must be managed and handled strictly in accordance with the General Data Protection Regulations, the Data Protection Act 2018 and the Criminal Procedure and Investigations Act 1996. Make sure you handle and manage any material properly and in accordance with these and any other statutory or other requirements that may apply from time to time. This material or information should also be handled in line with the Designated Person's recommendations detailed within the application. Failure to do so may render the product inadmissible as evidence as well as exposing the Council to risk.

3.9 All of the forms referred to in this procedure must be typed and signed. The copying and pasting of stock phrases is not permitted. The authorisation has to be tailor-made to suit the specific risks and circumstances of the intended surveillance operation. Make sure that you use the latest versions of the form you need by going to the appropriate link on the Home Office website.

4. SCOPE OF PROCEDURE

4.1 This Part of the Council's Procedure applies to all officers of the Council wishing to secure the acquisition and disclosure of Communications Data.

4.2 Unless there is alternative legal authority, the Council's approach to the acquisition and disclosure of Communications Data is to comply with this Procedure, and therefore RIPA, and also to have regard to and comply with the Code of Practice as well as any procedures or guidance issued by the IOCCO.

4.3 **It is critical that you understand that the Council, other than in its capacity as Fire and Rescue Authority, can only carry out the**

Communications Data activities to which this Part relates where it is necessary for the prevention or detection of crime. Save in its capacity as Fire and Rescue Authority, the Council cannot use these powers for any other purpose.

The lawful reason for the Fire and Rescue Authority to conduct surveillance is:

- **For the purpose of preventing and detecting crime or for the purpose of preventing disorder;**
- **In the interests of public safety.**

4.4 The acquisition of Communications Data under the Act will be a justifiable interference with an individual's human rights under Article 8 of the HRA only if the conduct being authorised or required to take place is both necessary and proportionate and in accordance with the law. Importantly only Communications Data within the meaning of Section 21(4) of the Act may be acquired for these purposes.

4.5 To acquire Communications Data approval authorisation must be obtained from a Designated Person in accordance with this procedure and subsequently from a Justice of the Peace and they will not grant authorisation unless the acquisition is:

- **NECESSARY** for the purpose of preventing or detecting crime. Section 81(5) of RIPA provides that detecting crime shall be taken to include, inter alia, establishing by whom, for what purpose, by what means and generally in what circumstances any crime was committed; and

- **PROPORTIONATE** to what is sought to be achieved by accessing the Communications Data. When filling in this part of the authorisation request have regard to the prompts set out in the request which relate to:

    - why accessing the Communications Data is proportionate to what it seeks to achieve;
    - how intrusive it might be on the subject of the activity or on others;
    - why the intrusion is outweighed by the need for surveillance in operational terms or whether the evidence be obtained by any other means.

- In addition, measures must be taken where practicable to avoid or minimise so far as practicable Collateral Intrusion or intended intrusion.

Prior to submission to a NAFN the Designated Person must be certain that the following elements of balancing proportionality have been properly considered:

  - balancing the size and scope of the proposed activity against the gravity and extent of the perceived crime or offence – is the proposed acquisition a "sledgehammer to crack a nut" having regard to the Council's regulatory purpose? If it is, it is probably not proportionate;
  - explaining how and why the methods to be adopted will cause the least possible intrusion on the subject and others, whether collateral or intended;
  - considering whether the activity is an appropriate use of the legislation and a reasonable way, having considered all reasonable alternatives, of obtaining the necessary result – if there are other practical ways of getting the information they should be explored;
  - evidencing as far as reasonably practicable what other methods have been considered and why they were not implemented – is the proposed authorisation/notice the only practical way of obtaining the required information? If it is not then alternative methods of obtaining the information should be explored.

The Designated Person ought also to consider whether the accessing of the Communications Data is likely to add anything to the investigation or operation and whether the resulting intelligence or evidence will significantly benefit the enquiry or chance of prosecution.

The Designated Person is likely to be a key witness in any challenge to the use of the RIPA procedures and so ensuring the proper consideration of all relevant issues and the recording of that consideration is fundamentally important.

4.6 If the proposed actions do not fall within these definitions, or there is alternative legal authority for their use, then there is no requirement to follow this procedure. This means that you should either not be carrying out the surveillance or there is no need for an authorisation. Do not assume that you can simply proceed with the acquisition of

Communications Data if this Procedure does not seem to apply. If in doubt get advice from the Senior Responsible Officer or the Monitoring Officer.

5. APPLICATIONS

5.1 An Applicant who requires access to Communications Data must initially complete and submit the application form to a SPoC. This must be carried out through NAFN's online application process. The Applicant should seek advice from the SPoC in the completion of the application form given that the SPoC will be accredited having undertaken training specifically relating to this function and can give informed advice in relation to the application.

It is critically important that the extent of the proposed Communications Data acquisition is fully explained on the authorising form because the authorisation only permits the activities stated upon it. Anything beyond what is authorised will, prima facie, be unlawful.

5.2 The SPoC will check the application form and if correctly completed will forward it to a Designated Person prior to submission to a Justice of the Peace, having completed the section for assessment by the SPoC.

5.3 If the application is deficient the SPoC will return the application to the Applicant identifying all the deficiencies within the application and allow the applicant to revise the form for re-submission.

5.4 Once an application is forwarded by a SPoC to a Designated Person the Designated Person will consider the application form, including necessity, proportionality and collateral intrusion and will complete the relevant section of the form. Any requested authorisation will be appropriate where the CSP allows the Council to obtain the information itself (e.g. where the Council has access to the CSP's database) or in any event where it is considered that a notice is not appropriate.

5.5 The authorisation will be valid for a period of one month from the date of authorisation.

5.6 If it is considered appropriate the Designated Person will prepare a notice requiring the provision of data by the CSP.

Use the form with the name **'Comms Notice'**.

5.7 It is unlikely that the Council will be in a position to take advantage of an authorisation to obtain Communications Data and so the normal course upon approval of an application will be for the Designated Person to issue a notice to the CSP. If an authorisation to acquire is granted by a Justice of the Peace the form with the name **'Comms Schedule'** will need to be used.

5.8 The notice or authorisation will be valid for a period of one month from the date of the approval by a Justice of the Peace.

5.9 Once verified by the Designated Person will then send the application to NAFN. The Designated Person must tell NAFN, who should receive the data which is obtained. NAFN will retain the completed authorisation form and if appropriate serve the notice on the CSP. Communication with the CSP must only be carried out NAFN. NAFN are issued with a unique PIN code which allows them to approach the CSP. The CSP is obliged to supply the requested data when a notice is served and the CSP is responsible for checking that NAFN is accredited prior to providing the Communications Data.

5.10 The SPoC will receive the data from the CSP and forward it in accordance with the Designated Person's instructions. The recipient of the data, usually the Applicant, must retain it in its original form. The SPoC will also retain a copy of the obtained data in its original form.

5.11 CSP's can, upon receiving a request from the SPoC, provide witness statements for use in court proceedings where data has previously been obtained during the investigation procedure. Evidential statements should be requested at the earliest opportunity if required in a not guilty case. The date of the pre-trial review and trial shall be provided by NAFN to the witness(es) who shall in turn provide dates of unavailability as necessary. The Applicant shall immediately inform NAFN when the plea is changed to guilty or the case otherwise ends before a trial takes place.

5.12 Any errors that come to light will immediately be addressed by NAFN and the required notification given to the Interception of Communications Commissioners Office (IOCCO). An error can only occur after a Justice of the Peace has granted an authorisation and the acquisition of data has been initiated, or has given notice and the notice has been served on a CSP in writing, electronically or orally. Errors might occur, for example:

- An authorisation or notice made for a purpose, or for a type of data, which the relevant public authority cannot call upon, or seek, under the Act;
- Human error, such as incorrect transposition of information from an application to an authorisation or notice;
- Disclosure of the wrong data by a CSP when complying with a notice;
- Acquisition of the wrong data by a public authority when engaging in conduct specified in an authorisation.

5.13 As appropriate, use the forms with the names **'Comms error Reporting by Public Authority'** or **'Comms error Reporting by CSP'**.

5.14 Additionally, the application should record subsequently whether it was approved or not by a Designated Person prior to submission to a Justice of the Peace, and by whom and when that decision was made. If approved, the application form should, to the extent necessary, be cross referenced to any authorisation granted by a Justice of the Peace or notice given.

5.15 As NAFN is the Council's only SPoC there is no need for the Council to ensure that there are Accredited SPoCs within the Council.

6. PROCEDURE FOR APPLYING FOR APPROVAL

6.1 Following verification by the Designated Person the first stage of the process in applying for approval is for the local authority to contact NAFN.

6.2 NAFN will be provided with the Application and a copy of the Communications Data authorisation/notice setting out the case. This should contain all information that is relied upon. For Communications Data requests the notice may seek consequential acquisition of specific subscriber information. The necessity and proportionality of consequential acquisition will be assessed by the NAFN as part of their consideration.

6.3 Although the Council is required to provide a brief summary of the circumstances of the case in the judicial application, this is supplementary to and does not replace the need to supply the original authorisation as well.

6.4 The order will be completed by NAFN and will be forwarded to OCDA for

authorisation.

7. NOTICE CANCELLATION AND WITHDRAWAL OF AUTHORISATIONS

7.1 A Designated Person who has given notice to a CSP shall cancel the notice if, at any time after giving the notice, it is no longer necessary for the CSP to comply with the notice or the conduct required by the notice is no longer proportionate to what was sought to be achieved.

7.2 Reporting the cancellation of a notice to a CSP shall be undertaken by the Designated Person directly or on their behalf by the SPoC. Where human rights considerations are such that a notice should be cancelled with immediate effect the Designated Person or the SPoC will notify the CSP.

7.3 Cancellation of a notice reported to a CSP must:

- *be* undertaken in writing or, if not, in a manner that produces a record of the notice having been cancelled;
- identify, by reference to its unique reference number, the notice being cancelled;
- record the *date and, when appropriate to do so, the time when the notice was cancelled.*

7.4 In cases where the SPoC has initiated the cancellation of a notice and reported the cancellation to the CSP, the Designated Person must confirm the decision in writing for the SPoC or, if not, in a manner that produces a record of the notice having been cancelled by the Designated Person. Where the Designated Person who gave the notice to the CSP is no longer available, this duty should fall on the person who has taken over their role.

7.5 Where a Designated Person considers an authorisation should cease to have effect, because the conduct authorised becomes unnecessary or no longer proportionate to what was sought to be achieved, the authorisation must be withdrawn. This may be done by the SPoC but they must then inform the Designated Person who granted the authorisation.

7.6 Withdrawal of an authorisation should:

- *be* undertaken in writing or, if not, in a manner that produces a record of it having been withdrawn
- identify, by reference to its unique reference number, the authorisation being withdrawn
- record the date and, when appropriate to do so, the time when the authorisation was cancelled
- record the *name and the office, rank or position held by the Designated Person informed of the withdrawal of the authorisation*

7.7 When it is appropriate to do so a CSP should be advised of the withdrawal of an authorisation, for example where details of an authorisation have been disclosed to a CSP.

8. PAYMENT

8.1 RIPA provides for payment to be made by the Council to the CSP to compensate if for the costs of complying with a notice. The SPoC will obtain the information of the cost of obtaining information and inform the Applicant and the Designated Person.

8.2 The SPoC will be responsible for arranging payments to the CSP.

9. RECORD KEEPING AND DATA PROTECTION

9.1 All records referred to in this procedure will be retained for a period of five years from the ending of the authorisation or last renewal. These records will be kept in a secure file, with access limited to the appropriate officers. Unlike records relating to directed surveillance and CHIS, records relating to the acquisition and disclosure of Communications Data will be held centrally by the SPoC. These records must be available for inspection by the Commissioner and retained to allow the Investigatory Powers Tribunal to carry out its functions.

9.2 The records that will be kept will include the date and, when appropriate to do so, the time when each notice or authorisation is given or granted, renewed or cancelled and must also include a record of the following items:

- number of applications submitted to a Designated Person for a decision as to whether to submit an application to the Justice of the Peace to obtain Communications Data;
- number of notices requiring disclosure of Communications Data

within the meaning of each subsection of section 21(4) of RIPA or any combinations of data; and

- number of authorisations for conduct to acquire Communications Data within the meaning of each subsection of section 21(4) of RIPA or any combinations of data.

9.3 As appropriate, the authority's data protection advisors will be consulted to ensure that material is handled, stored and disposed of in accordance with the requirements of the General Data Protection Regulations and the Data Protection Act 2018. In addition, the requirements of the Criminal Procedures and Investigations Act 1996 must be complied with.

9.4 The SPoC will retain a copy of the obtained data in its original form.

9.5 All records maintained under RIPA must be kept secure and confidential.

9.6 The proper keeping of records, including the central record, is also important for the quarterly reporting that is required to Members on the amount and nature of the use of RIPA that has occurred and also to allow Members to effectively consider the confirmation or variation, as appropriate and if necessary, of this Procedure on an annual basis as required by the Code of Practice.

10. GENERAL

10.1 This Procedure is a public document and will be available for public inspection at Old Wesleyan Chapel, Garrison Lane, St Mary's, Isles of Scilly, TR21 0JD and on the Council's website. Copies of this Procedure will be available to staff on the intranet. The procedure will be reviewed and updated from time to time by the Senior Responsible Officer and Monitoring Officer in consultation with appropriate colleagues and referred to Members, as appropriate, for approval.

10.2 Complaints concerning the way in which the Council has operated this procedure may be made to the Chief Executive, Council of the Isles of Scilly, Old Wesleyan Chapel, Garrison Lane, St Mary's, Isles of Scilly, TR21 0JD or through the complaints system available on the Council's website.

10.3 Oversight of Communications Data procedures is provided by the investigatory Powers Commissioner's Office who may be contacted at PO Box 29105, London, SW1V 1ZU.

PART 3
SURVEILLANCE OUTSIDE OF THE SCOPE OF RIPA – (NON-RIPA SURVEILLANCE)

BACKGROUND

1.1 Amendments to the Regulation of Investigatory Powers (Directed Surveillance and Covert Human Intelligence Sources) Order 2010 mean that a local authority can now only grant an authorisation under RIPA for directed surveillance where the local authority is investigating criminal offences which attract a maximum custodial sentence of at least six months (the serious crime threshold) or criminal offences relating to the underage sale of alcohol or tobacco.

1.2 Notwithstanding these changes it is envisaged that surveillance may be required which falls outside of RIPA, for example in the case of anti-social behaviour offences which do not meet the serious crime threshold, or the monitoring of social media sites for employment or social care matters.

1.3 The Office of Surveillance Commissioners Procedures and Guidance 2016 states that it is prudent to maintain an auditable record of decisions and actions to use surveillance outside of, and therefore without the protection of, RIPA and that such activity should be regularly reviewed by the SRO. The SRO for RIPA will therefore have oversight of Non-RIPA surveillance to ensure that such use is compliant with human rights legislation, that risks are being properly assessed and that the use of such surveillance is otherwise appropriate. In addition to this, the SRO will maintain a central record of Non-RIPA surveillance.

1.4 It should be noted that reviewing open source sites does not require authorisation unless the review is carried out with some regularity, usually when creating a profile, in which case direct surveillance authorisation will be required. Note the definition of online covert activity at the start of this policy.

1.5 If it becomes necessary to breach the privacy controls and become, for

example, a ‘friend’ on sites such as Facebook, with the investigating officer utilising a false account that conceals their identity as a Council officer in order to allow them to gather information, this is then a covert operation and should be authorised, as a minimum, as directed surveillance. If the person gathering the information engages in any form of relationship with the account operator, then they become a CHIS requiring authorisations such as management by a Controller and Handler with a record being kept and a risk assessment created.

1.6 **DO NOT** assume that the direct surveillance you are undertaking either does not need an authorisation or is not RIPA surveillance. You must check and if you are in doubt you should contact the Senior Responsible Officer or the Monitoring Officer.

2. PROCEDURE

2.4 All Non-RIPA Surveillance must be authorised in advance using the following procedure:

2.4.1 A URN is to be obtained from the central team using the email address surveillance@cornwall.gov.uk;

2.4.2 The application should be made using the standard RIPA application form which must be clearly annotated at the top of the first page with ‘NON-RIPA SURVEILLANCE’;

2.4.3 All sections of the application form must be completed by the officer seeking authorisation (applicant), as if it were an application for authorisation to undertake RIPA surveillance. This approach will ensure that the applicant considers all relevant issues including the detail of the surveillance, who will be impacted, over what period the surveillance should be undertaken, proportionality and necessity. The applicant should also consider if it is necessary to complete a risk assessment and, if this is required, the standard RIPA risk assessment form is to be used. If it is determined that no risk assessment is required a file note is to be made to detail why not and that file note must be copied to surveillance@cornwall.gov.uk;

2.4.4 The application form then must be submitted for authorisation to a manager at a level no lower than tier 4 (Chief Executive (tier 1), or Strategic Director (tier 2). There is no need to apply for judicial

approval; and

2.4.5 Whether or not the application is authorised a copy of the completed and signed application form must be passed to the central team using surveillance@cornwall.gov.uk.

2.5 For all Non-RIPA Surveillance the procedures applied to reviews, renewals and cancellations must also be followed but in the context of the surveillance falling outside of RIPA. The role of the Authorising Officer will be undertaken by the relevant manager as identified in paragraph 2.4.4 above.

2.6 The authorisation or refusal of the request, the outcome of any reviews, renewal applications and the eventual cancellation of the authorisation must be notified to the central team using surveillance@cornwall.gov.uk by copying the relevant documentation to them.

3. RECORD KEEPING

3.1 All records referred to in this procedure will be retained for a period of five years from the ending of the authorisation or last renewal. These records will be kept in a secure file, with access limited to the appropriate officers.

3.2 Material will be handled, stored and disposed of in accordance with the requirements of the General Data Protection Regulations and the Data Protection Act 2018.

APPENDIX A

Even though those who may be authorising officers for the purposes of RIPA are prescribed in regulations, the Council will be limiting those within the authority who may authorise applications for submission to a Justice of the Peace. Until such time as those officers are identified and specified in this Appendix the Council will be relying on the designations in the regulations. No other person may authorise a submission to a Justice of the Peace. Authorising officers are not restricted to authorising, or refusing, applications for applicants from their own service area as it is the Council's intention that the traditional service boundaries should be broken down in this respect.

Authorising Officers

These officers are:

- Kevin Brader, Head of Public Health and Protection, Cornwall Council

Authorised Officers in relation to Confidential material

- Russell Ashman, Chief Executive, Council of the Isles of Scilly
- Officer deputising for the Chief Executive but only in their absence

Designated Persons

Those persons who have been designated as Authorising Officers as above

Single Point of Contact

National Anti-Fraud Network (NAFN)

Senior Responsible Officer

Simon Mansell, Data Protection Officer, Council of the Isles of Scilly