

Policy Title: Corporate Policy and Procedure on the Regulation of Investigatory Powers Act 2000 (RIPA)

ID	<i>Counter Fraud -RIPA</i>
Last Review Date	<i>November 2023</i>
Next Review Date	<i>When any changes in personnel, legislation or Codes of Practice</i>
Approval	<i>Governance and Audit and Standards Committee.</i>
Policy Owner	<i>Elizabeth Goodwin, Chief Internal Auditor & Senior Responsible Officer for RIPA</i>
Policy Author	<i>Paul Somerset (Deputy Chief internal Auditor & Authorising Officer)</i>
Advice & Guidance	<i>Paul Somerset, Tel: 023 9284 4673 Deputy Chief Internal Auditor paul.somerset@portsmouthcc.gov.uk</i>
Location	<i>Policy Hub</i>
Related Documents	<i>Covert Surveillance and Property Interference Code of Practice 2018; Covert Human Intelligence Sources Code of Practice 2022; Communications Data Code of Practice 2018; Regulation of Investigatory Powers Act 2000; Investigatory Powers Act 2016; Protection of Freedoms Act.</i>
Applicability	<i>All PCC Staff & Contractors (acting on behalf of the Authority, i.e., an agent)</i>

Summary:

1. Controls on covert surveillance were introduced as a consequence of the Human Rights Act 1998, which enshrined the European Convention and Human Rights into UK law and came into effect on 2 October 2000.
2. The Regulation of Investigatory Powers Act 2000 (RIPA), RIPA (Directed Surveillance and Covert Human Intelligence Sources) Order 2010 and **The Investigatory Powers Act 2016 (IPA)** aim to ensure that public bodies respect the privacy of members of the public when carrying out their investigations and that there is an interference with privacy only where the law permits it and there is a clear public interest justification in the prevention or detection of crime.
3. The Protection of Freedoms Act 2012 requires that Local Authorities seeking RIPA authorisation are subject to judicial approval. This means that approval of the RIPA authorisation or renewal of an authorisation must be approved by a judicial authority in the local Magistrates Court.
4. The Regulation of investigatory Powers (Directed Surveillance and Covert Human Intelligence Sources) (Amendment) Order 2012 has stated that RIPA can only be used for criminal offences that could attract a custodial sentence of 6 months or more or are related to the **underage sale of alcohol and tobacco or nicotine inhaling products**, Local Authorities can only consider applications in the context of prevention & detection of crime. **Local authorities cannot authorise directed surveillance for the purpose of preventing disorder unless this involves a criminal offence(s) punishable by a maximum term of at least 6 months' imprisonment. Local authorities may therefore continue to authorise the use of directed surveillance in more serious cases providing the other tests are met – i.e., that it is necessary and proportionate and where prior approval from a JP has been granted.**
5. RIPA controls the use of various methods of investigation, in particular the use of covert surveillance, covert human intelligence sources (CHIS). **The IPA controls the use of methods for accessing communication data. RIPA & IPA both define what constitute these activities.**
6. If the activities proposed by investigating officers fall within the terms of RIPA **and/or IPA** (see Section 3) then this policy, procedures and the **relevant** Code of Practice must be followed. If investigating officers have any doubts about the application or meaning of its provisions, they must obtain advice from the Authorising Officers before proceeding. (see Appendix A)
7. RIPA is not concerned with overt surveillance. Most of the surveillance carried out by or on behalf of Portsmouth City Council will be overt. That is, there will be nothing secretive, clandestine, or hidden about it. In many cases for officers, it will be business as usual i.e., going about Council business openly e.g., a Trading Standards Officer visiting a market to look for sales of counterfeit goods. Where it is targeted, that is a specific stall holder is to be the focus of covert surveillance, it becomes directed surveillance and requires a RIPA authorisation.
8. All directed surveillance, use of a CHIS, or **acquisition of** communications data must be properly authorised. Failure to secure proper authorisation or to comply with this procedure could lead to evidence being excluded by the court, significant costs being awarded against the City Council and complaints against the City Council. The City Council is subject to audit and inspection by the Investigatory Powers Commissioners Office (IPCO) and it is important that compliance with RIPA and with the Guide can be demonstrated in every case.

Contents

1. Policy Statement
2. Objectives
3. Terms explained
4. Procedure
5. CHIS (Covert Human Intelligence Sources)
6. CCTV & Aerial Covert Surveillance
7. Communications Data
8. Non-RIPA Surveillance
9. Record Keeping & Error Reporting
10. Product Management Process
11. Impact Risk Assessment
12. Further Guidance
13. Oversight
14. Complaints

[Appendix A: List of Authorised Persons](#)

[Flowchart 1: Surveillance, guidance.](#)

[Flowchart 2: CHIS guidance.](#)

[Flowchart 3: Accessing communications data](#)

[Impact Risk Assessment Form](#)

[Surveillance an aid to investigation](#)

[RIPA Application for Directed Surveillance](#)

[RIPA Application review form](#)

[RIPA Cancellation Form](#)

[Application for judicial approval for authorisation to obtain or disclose communications data, to use a covert human intelligence source or to conduct directed surveillance.](#)

[Regulation of Investigatory Powers Act 2000 sections 23A, 23B, 32A, 32B.](#)

Further information including forms and codes of practice:

<http://www.homeoffice.gov.uk/counter-terrorism/regulation-investigatory-powers/ripa-codes-of-practice/>

<https://www.gov.uk/government/collections/ripa-codes>

1. Policy Statement

- 1.1 In some circumstances, it may be necessary for Portsmouth City Council employees or contractors, in the course of their duties, to make observations of a person or person(s) in a covert manner, i.e., without that person's knowledge. By their nature, actions of this sort may constitute an interference with that person's right to privacy and may give rise to legal challenge as a potential breach of Article 8 of the European Convention on Human Rights and the Human Rights Act 1998 ('the right to respect for private and family life').
- 1.2 The Regulation of Investigatory Powers Act (2000) [RIPA] provides a legal framework for covert surveillance activities by public authorities, (including local authorities), and an independent inspection regime to monitor these activities.
- 1.3 Portsmouth City Council employees and contractors (where applicable) will adhere to the authorisation procedure before conducting any covert surveillance and if in doubt will seek advice from an Authorising Officer.
- 1.4 Employees and contractors (where applicable) of Portsmouth City Council will **not** carry out intrusive surveillance within the meaning of the Regulation of Investigatory Powers Act 2000 [refer to Terms Explained Section 3 paragraph 3.7] nor will they interfere with property or wireless telegraphy.
- 1.5 Officers of Portsmouth City Council may only authorise or engage in covert surveillance, CHIS, and access to communication data to prevent or detect criminal offences that are either punishable, whether on summary conviction or indictment, by a maximum term of at least 6 months' imprisonment or are related to the underage sale of alcohol and tobacco or nicotine inhaling products. The Council cannot authorise directed surveillance for the purpose of preventing disorder **unless** this involves a criminal offence(s) punishable by a maximum term of at least 6 months' imprisonment. Portsmouth City Council may continue to authorise use of directed surveillance in more serious cases as long as the other tests are met – i.e., that it is necessary and proportionate and where prior approval from a JP has been granted.
- 1.6 This Policy makes a number of references to confidential information. The revised Covert Surveillance and Property Interference Code of Practice, which was revised in August 2018, the CHIS Code of Practice revised in December 2022, and the Communications Data Code of Practice which came into effect in November 2018 each require the highest levels of authorisation where 'confidential information' is likely to be acquired and at Portsmouth City Council this is the Chief Executive. [Refer to Definitions in Section 3]
- 1.7 **Portsmouth City Council** will make arrangements to ensure that the relevant Code of Practice is complied with, including having Member and Senior Officer oversight to ensure that compliance and the appropriate training is given to officers.
- 1.8 Statutory Instrument 2010 No 521 restricts authorising officers in local authorities to prescribed offices of no lower a level than **Director, Head of Service, Service Manager or equivalent.**

2. OBJECTIVES

- 2.1 The objective of this Policy and Procedures is to ensure that all work involving directed surveillance by Portsmouth City Council employees is carried out effectively, while remaining in accordance with the law. It should be read in conjunction with the Regulation of Investigatory Powers Act (2000), RIPA (Directed Surveillance and Covert Human Intelligence Sources) Order 2010, **the Investigatory Powers Act 2016**, The Protection of Freedoms Act 2012 and the **relevant** Code of Practice on Covert Surveillance, Use of Covert Human Intelligence Sources and **Communications data**.

3 TERMS EXPLAINED

- 3.1 **Authorising Officer** is the person(s) in the Organisation who is entitled to give an authorisation for directed surveillance, **use of CHIS, and approvals of applications for acquisition of communications data** in accordance with RIPA, **IPA, and relevant Code of Practice**. For covert surveillance and use of CHIS prior approval by a Magistrate is required before any activity can begin.
- 3.2 **CHIS (Covert Human Intelligence Source)**. A CHIS is someone who establishes or maintains a relationship with a person for the purpose of covertly obtaining or disclosing information. In practice, this is likely to cover the use of an informant, volunteer, or Council officer in striking up a relationship with someone as part of an investigation to obtain information “under cover”.
- 3.3 Someone who volunteers information to Portsmouth City Council, either as a complainant or out of civic duty, is not likely to be a covert human intelligence source. i.e., if someone is keeping a record, say, of neighbour nuisance, this will not itself amount to the use of a CHIS. The use of a CHIS consists of any action on behalf of the Council to induce, ask or assist a person to engage in the conduct of a CHIS, or to obtain information by means of the conduct of a CHIS. In addition, Officers need to consider whether any information passed to the Council has been obtained in the course of a personal or other relationship, such as a relative, friend or work colleague, even if that relationship was not established or maintained for the purpose of obtaining it. In this event advice should be sort immediately from an Authorising Officer.
- 3.4 **Collateral intrusion** means the obtaining of private information about persons who are not the intended subject of the surveillance. This could include their family, colleagues, and associates, anyone who is seen with and interacts with the subject during the surveillance operations. The fact that covert surveillance occurs in a public place or on business premises does not mean that it cannot result in the obtaining of private information about a person.
- 3.5 Every effort should be made to minimise unnecessary intrusion, however, where collateral Intrusion is unavoidable, the identified risk must be recorded for consideration on the RIPA application so that a proportionality test can be applied.
- 3.6 For example, prolonged surveillance targeted on a person will undoubtedly result in the obtaining of private information about him/her and others that he/she

comes into contact, or associates, with. However, strict rules must be complied with before such surveillance may be authorised.

- 3.7 Similarly, although overt, public space CCTV cameras do not normally require authorisation. If however the camera is tasked for a specific purpose, which involves targeted surveillance on a particular person, or a group of people, authorisation must be obtained.
- 3.8 **Confidential Material** Confidential information consists of matters subject to legal privilege, confidential personal information, or confidential journalistic material, or where information identifies a journalist's source, where material contains confidential personal information or communications between Members of Parliament and another person on constituency business. So, for example, extra care should be given where, through the use of surveillance, it would be possible to acquire knowledge of discussions between a minister of religion and an individual relating to the latter's spiritual welfare, or where matters of medical or journalistic confidentiality or legal privilege may be involved.
- 3.9 **Covert surveillance Covert (or 'hidden') surveillance.** Covert surveillance is carried out in a manner calculated to ensure that the person subject to the surveillance is not aware it is taking place. That is, it is done secretly.
- 3.10 **Directed surveillance** Surveillance is undertaken if the following are all true:
- it is covert, but not intrusive surveillance,
 - it is conducted for the purposes of a specific investigation or operation,
 - 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),
 - it is conducted otherwise than by way of an immediate response to events or circumstances, the nature of which is such that it would not be reasonably practicable for an authorisation to be sought.

Thus, the planned covert surveillance of a specific person, where not intrusive, would constitute directed surveillance if such surveillance is likely to result in the obtaining of private information about that, or any other person. (*Please note - "private information" is explained at 3.14 below*).

- 3.11 **Intrusive Surveillance** This is covert surveillance of anything taking place on residential premises or in a private vehicle that involves the presence of an individual on the premises or in the vehicle, or is carried out by means of a surveillance device capable of providing information of the same quality and detail as might be expected to be obtained from a device actually present on the premises or in the house.

Only the police and certain other law enforcement agencies may carry out intrusive surveillance. Council officers, or anyone on behalf of the Council, **must not** carry out intrusive surveillance.

An example of intrusive surveillance is planting a listening or other device ('bug') in a person's home or in their private vehicle or using a

sophisticated listening device (eg. DAT) outside a person's home or in their private vehicle that will provide results equivalent to being "on-site". N.B. Interference with property or wireless telegraphy is also forbidden to the Council.

- 3.12 **Necessity.** An authorisation for Directed Surveillance and or CHIS by Portsmouth City Council is necessary if it is for the purpose of preventing or detecting crime.
- 3.13 **Overt (or 'open') surveillance.** Surveillance will be overt if the subject has been told that it will happen. Note: you do have to be careful however about obtaining private information on others that have not been informed. Examples of overt surveillance are,
- Police Officer, Street Warden, Enforcement Officer, or Ranger on routine patrol
 - Sign-posted public space CCTV cameras (in normal use)
 - Recording noise coming from outside the premises, after the occupier has been warned in writing, that this will occur if the noise persists.
 - An Officer may act overtly when test purchasing as there is no forming of a relationship with the retailer (i.e., the officer behaves no differently from a normal member of the public).
 - CCTV cameras providing general traffic crime or public safety information
- 3.14 **Private information** includes any information relating to a person's private or family life. As a result, private information is capable of including any aspect of a person's private or personal relationship with others, such as family and professional or business relationships. Information which is non-private may include publicly available information such as books, newspapers, journals, TV and radio broadcasts, newswires, web sites, mapping imagery, academic articles, conference proceedings, business reports, and more. Such information may also 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 a member of the public.
- 3.15 **Private vehicle** means any vehicle that is used primarily for the private purpose of the person who owns it or of a person otherwise having the right to use it. This does not include a person whose right to use a vehicle derives only from his having paid, or undertaken to pay, for the use of the vehicle and its driver for a particular journey. A vehicle includes any vessel, aircraft, or hovercraft.
- 3.16 **Proportionality** involves balancing the seriousness of the intrusion into the privacy of the subject of the operation (or any other person who may be affected) against the need for the activity in investigative and operational terms. The fact that a suspected offence may be serious will not alone render the proposed actions proportionate. Similarly, an offence may be so minor that any deployment of covert techniques would be disproportionate. No activity should be considered proportionate if the information which is sought could reasonably be obtained by other less intrusive means.
- 3.17 **Residential premises** means any premises occupied or used, however temporarily, for residential purposes or otherwise as living accommodation.

- 3.18 **Surveillance** is monitoring, observing, or listening to persons, their movements, their conversations or other activities or communications; recording anything monitored, observed or listened to in the course of surveillance; or Surveillance by or with the assistance of a surveillance device.

4. THE PROCEDURE

Scope

- 4.1 This procedure applies in all cases where `directed surveillance` is being planned or carried out. Directed surveillance is defined in the code of Practice as surveillance undertaken "for the purposes of a specific investigation or operation" and "in such a manner as is likely to result in the obtaining of private information about a person" for the prevention and detection of crime.
- 4.2 The procedure does not apply to:
- Ad-hoc covert observations that do not involve the systematic surveillance of specific person(s)
 - Observations that are not carried out covertly, or
 - Unplanned observations made as an immediate response to events
- 4.3 In cases of doubt, the authorisation procedures described below should be followed.

Test Purchases

- 4.4 An impact assessment prior to covert test purchases being made should be carried out **and the Age-Related Sales - Code of Practice 2014 followed**. If the test purchase is simply entering a business premise, making a purchase and leaving then it is unlikely to require a RIPA. Where any service wishes to carry out covert operations that they try to make overt, by writing to vendors in advance of an operation, they should write to vendors no more than two weeks in advance. Any more than this and it may be construed as covert surveillance and an impact assessment/ RIPA authorisation may be required.

Children as Juvenile Sources

- 4.5 Special safeguards must be put in place when test purchases are being made by children (anyone under 18 years of age). **Any consideration to using a child as a CHIS must include reference to Chapter 4 of CHIS Code of Practice 2022. Children should only be authorised to act as CHIS in exceptional circumstances and subject to an enhanced risk assessment process. The need to safeguard and promote the best interests of the child is a primary consideration in all such CHIS deployments, both when deciding whether to grant the authorisation and during the conduct of any subsequent operation.**

Note: Children should only be authorised to act as CHIS in exceptional circumstances and subject to the enhanced risk assessment process set out in Article 5 of the Juveniles Order. Portsmouth City Council has in place existing child safeguarding guidance, policies and procedures of general application, and have regard to these if a child as juvenile sources is ever considered.

Note: PCC should ensure that before authorising a child as a CHIS it has in place existing child safeguarding guidance, policies and procedures of general application, and regard should be had to these where relevant.

Drive Bys

- 4.6 Where an officer, as part of an investigation, intends to drive by a property to establish the location of a property then a RIPA is unlikely to be required however if the drive by is to assess for signs of occupation and a record is made it is likely a RIPA will be required. An impact risk assessment should be completed initially and if it shows that collateral intrusion is likely to arise a full RIPA application should be made prior to any activity.

Online Covert Activity.

- 4.7 The Home Office revised Code of Practice 3.10 to 3.17 states:
'The growth of the internet, and the extent of the information that is now available online, presents new opportunities for public authorities to view or gather information which may assist them in preventing or detecting crime or carrying out other statutory functions, as well as in understanding and engaging with the public they serve. It is important that public authorities are able to make full and lawful use of this information for their statutory purposes. Much of it can be accessed without the need for RIPA authorisation; use of the internet prior to an investigation should not normally engage privacy considerations. But if the study of an individual's online presence becomes persistent, or where material obtained from any check is to be extracted and recorded and may engage privacy considerations, RIPA authorisations may need to be considered'.
- 4.7.1 'Where a person acting on behalf of a public authority is intending to engage with others online without disclosing his or her identity, a CHIS authorisation may be needed'. In deciding whether online surveillance should be regarded as covert, consideration should be given to the likelihood of the subject(s) knowing that the surveillance is or may be taking place'.
- 4.7.2 'Depending on the nature of the online platform, there may be a reduced expectation of privacy where information relating to a person or group of people is made openly available within the public domain, however in some circumstances privacy implications still apply. This is because the intention when making such information available was not for it to be used for a covert purpose such as investigative activity. This is regardless of whether a user of a website or social media platform has sought to protect such information by restricting its access by activating privacy settings'.
- 4.7.3 'Where information about an individual is placed on a publicly accessible database, for example the telephone directory or Companies House, which is commonly used and known to be accessible to all, they are unlikely to have any reasonable expectation of privacy over the monitoring by public authorities of that information. Individuals who post information on social media networks and other websites whose purpose is to communicate messages to a wide audience are also less likely to hold a reasonable expectation of privacy in relation to that information'.
- 4.7.4 'Whether a public authority interferes with a person's private life includes a consideration of the nature of the public authority's activity in relation to that information. Simple reconnaissance of such sites (i.e., preliminary examination with

a view to establishing whether the site or its contents are of interest) is unlikely to interfere with a person's reasonably held expectation of privacy and therefore is not likely to require a directed surveillance authorisation. But where a public authority is systematically collecting and recording information about a particular person or group, a directed surveillance authorisation should be considered. These considerations apply regardless of when the information was shared online'.

4.7.5 'In order to determine whether a directed surveillance authorisation should be sought for accessing information on a website as part of a covert investigation or operation, it is necessary to look at the intended purpose and scope of the online activity it is proposed to undertake. Factors that should be considered in establishing whether a directed surveillance authorisation is required include:

- Whether the investigation or research is directed towards an individual or organisation.
- Whether it is likely to result in obtaining private information about a person or group of people.
- Whether it is likely to involve visiting internet sites to build up an intelligence picture or profile.
- Whether the information obtained will be recorded and retained.
- Whether the information is likely to provide an observer with a pattern of lifestyle.
- Whether the investigation or research is part of an ongoing piece of work involving repeated viewing of the subject(s).
- Whether it is likely to involve identifying and recording information about third parties, such as friends and family members of the subject of interest, or information posted by third parties, that may include private information and therefore constitute collateral intrusion into the privacy of these third parties.

4.8 Internet searches carried out by a third party on behalf of a public authority, or with the use of a search tool, may still require a directed surveillance authorisation.

4.9 The setting up of false identities is not allowed and an application and authorisation for the use and conduct of CHIS is necessary if a relationship is established or maintained.

Employee Investigations

4.10 For employment investigations of non-criminal activity if covert surveillance is proposed, a RIPA is not required. However, an assessment should always be made to ensure that it is lawful, collateral intrusion is minimised and the action is proportionate and necessary.

Confidential Material

4.11 Applications where there is a reasonable likelihood of acquiring confidential material will always require the approval of the Chief Executive. In reality this is likely to be very rare due to the nature of the Council's work, which is unlikely to conduct the sort of investigations whereby confidential material could be obtained but it must be considered at the outset.

4.12 Confidential material consists of:

- Matters subject to legal privilege, (for example between professional legal advisor and client)
- Confidential personal information, (for example relating to a person's physical or mental health), or
- Confidential journalistic material or where material identifies a journalist's source, or
- Confidential constituent information relates to communications between a Member of Parliament and a constituent in respect of constituency business.

Juvenile or vulnerable Adult CHIS's

- 4.13 Applications for CHIS using either Juveniles or vulnerable adults must be referred to the Chief Executive for Authorisation (See item 6).

Authorisation Procedure

- 4.14 Applications for directed surveillance will be authorised by either the Deputy Chief Internal Auditor or the Corporate Strategy Manager. The relevant Authorising Officer must see the process (from authorisation, review & cancellation) through for any applications they have authorised. If they are not able to do so because of sickness, then another authorising officer can continue with the process, but a record must be made of that fact.
- 4.15 There should never be a time when neither of the Authorising Officers are available due to unforeseen circumstances but if this should occur and the application for activity cannot wait for a week or so then the Senior Responsible Officer must designate an officer of suitable rank to act as an Authorising Officer and reasons for this and the absence of the Authorising Officers should be recorded. Under no circumstances can the Senior Responsible Officer act as Authorising Officer.
- 4.16 The Authorising officer should avoid authorising their own activities (i.e., where they are responsible for the activity or involved in the operation) wherever possible and only do so in exceptional circumstances. Where it becomes necessary to do so, a record to that effect must be made on the central record.
- 4.17 All applications for directed surveillance authorisations will be made on the official form. The applicant in all cases should complete this. They must demonstrate the who, what, why, where, when and how of an operation giving details of any and all technical equipment to be used and all options considered with reasons why this is the most reasonable and effective approach. Copying information from a previously authorised application is discouraged as it could be seen that insufficient thought has been applied and there is a danger of copying over incorrect information.
- 4.18 The proposed seizure of any items as part of the RIPA application must comply with PACE and relevant RIPA sections, although these will usually be in conjunction with the Police.
- 4.19 Once the RIPA application has been authorised the authorising officer will go through what has been authorised with the applicant in accordance with the ruling of R v Sutherland 2000. There must be no doubt about what has been

specifically authorised. The investigating officer can only carry out the actions that have been authorised in the RIPA application once approved by a Magistrate. It will be the Investigating Officer's responsibility to submit the application to the Magistrate following the Council's Authorising Officers' authorisation.

- 4.20 All requests to Magistrates will be on the forms as provided on the Home Office Website (<https://www.gov.uk/government/collections/ripa-forms>) The date when approved by the Magistrate is recorded on the Councils central record as well as the date authorised by the Authorising Officer.
- 4.21 All applications for directed surveillance renewals will be made on the official form (see link above 4.20). The applicant in all cases should complete this where the surveillance requires continuation beyond the previously authorised period (including previous renewals). Renewals must also be authorised by the authorising officer and approved by a Magistrate.
- 4.22 Portsmouth City Council will want to consider who is best able to answer the JP's questions on the policy and practice of conducting covert operations and the details of the case itself. It is envisaged that the case investigator will be able to fulfil this role. The investigator will know the most about the investigation and will have determined that the use of a covert technique is required to progress a particular case. (Ch 4 para 43 of the Home Office guidance to local authorities in England and Wales on the judicial approval process for RIPA and the crime threshold for directed surveillance) The case investigator must report back promptly to the Authorising Officer any comments made by the magistrate. Comments must be recorded by the Authorising Officer and action taken to incorporate or address them.
- 4.23 Where an authorisation ceases to be either necessary or appropriate the authorising officer will cancel an authorisation using the official form.
- 4.24 Any person giving an authorisation for the use of directed surveillance must set out in their own words why they believe the activity is necessary and proportionate stating that:
- Account has been taken of the likely degree of intrusion into the privacy of persons other than those directly implicated in the operation or investigation, (collateral intrusion). Measures or mitigation action have been taken, wherever practicable, to avoid unnecessary intrusion into the lives of those affected by collateral intrusion.
 - The authorisation is necessary.
 - The authorised surveillance is proportionate.
 - It is for a specific targeted criminal offence that carries a maximum sentence of 6 months or more, imprisonment, or is one of the exemptions.

Urgent Cases

- 4.25 There is no longer the power for Portsmouth City Council to make urgent oral authorisations. All authorisations, even if urgent, (where life or an operation is in jeopardy) must be in writing and approved by a magistrate. However, it is not

envisaged that there will be urgent cases as activities at PCC are unlikely to involve such scenarios.

Necessity

- 4.26 An authorisation for Directed Surveillance and/or CHIS is necessary if it is for the purpose of preventing or detecting crime.

Effectiveness

- 4.27 Surveillance operations shall be undertaken only by suitably trained or experienced employees, or under their direct supervision.

Proportionality

- 4.28 The use of surveillance shall not be excessive, i.e., it shall be in proportion to the significance of the matter being investigated and balance the intrusiveness of the activity on the target and others who might be affected by it against the need for the activity in operational terms. The activity will not be proportionate if it is excessive in the circumstances of the case or if the information which is sought could reasonably be obtained by other less intrusive means.

The following elements of proportionality should therefore be considered,

- balancing the size and scope of the proposed activity against the gravity and extent of the perceived crime or harm
- explaining how and why the methods to be adopted will cause the least possible intrusion on the subject and others,
- considering whether the activity is an appropriate use of the legislation and a reasonable way, having considered all reasonable alternatives, of obtaining the information sought,
- evidencing, as far as reasonably practicable, what other methods had been considered and why they were not implemented, or have been implemented unsuccessfully.

Authorisation

- 4.29 All directed surveillance shall be authorised in accordance with this procedure.

Time Periods - Authorisations

- 4.30 Written authorisations expire after 3 months from the day the activities were permitted to start, which is the day the JP / Magistrate approves the granting of the authority.

Review

- 4.31 The Authorising Officer should determine how often a review should take place of an authorisation and this should be as frequently as is considered necessary and practicable. A review of an authorisation should be undertaken regularly to

assess the need for the surveillance to continue. The results of the review are to be recorded on the central record.

Time Periods - Renewals

- 4.32 If at any time before an authorisation would expire, the Authorising Officer considers it necessary for the authorisation to continue for the purpose for which it was given, it may be renewed in writing for a further period of 3 months beginning with the day on which the previous authorisation ceases to have effect. Applications for renewal should only be made shortly before the authorisation is due to expire and must be submitted to a Magistrate by the Investigating Officer for judicial approval before they can be effective.
- 4.33 Any person entitled to authorise may renew authorisations. They may be renewed more than once, provided they continue to meet the criteria for authorisation and must be approved by a Magistrate to become effective.
- 4.34 All applications for the renewal of an authorisation for directed surveillance must record:
- Whether this is the first renewal or every occasion on which the authorisation has been renewed previously
 - Any significant changes to the information
 - The reasons why it is necessary to continue with the directed surveillance
 - The content and value to the investigation or operation of the information so far obtained by the surveillance
 - The results of regular reviews of the investigation or operation

Cancellation

- 4.35 The Authorising Officer who granted or last renewed the authorisation must cancel if they are satisfied that the directed surveillance no longer meets the criteria upon which it was authorised.
- 4.36 The cancellation should include how the surveillance assisted the investigation and details regarding direction of the product.

Monitoring

- 4.37 Each Service or discrete location within Services must maintain a record of all applications for authorisation, (including refusals), renewals, reviews, and cancellations.

Security and Retention of Documents

- 4.38 Documents created under this procedure are highly confidential and shall be treated as such. Services shall make proper arrangements for their retention, security and destruction, in accordance with the requirements of the Data Protection Act 1998 and the relevant Code of Practice.

- 4.39 The Chief Internal Auditor will be responsible for the creation and maintenance of an up-to-date Central Register of Authorisations containing the following information:
- The type of authorisation
 - The date the authorisation was given
 - Name and title of the authorising officer
 - The unique reference number of the investigation or operation
 - The title of the investigation or operation including a brief description and whether the urgency provisions were used and if so why
 - If the authorisation is renewed when it was renewed and who authorised including the name and title of the authorising officer
 - Whether the investigation or operation is likely to result in obtaining confidential information
 - The date the authorisation was cancelled and outcome
 - Whether or not it was self authorised i.e., authorised by an authorising officer involved in, or responsible for, the investigation or operation being authorised.
 - The date of Magistrates approval
- 4.40 The Chief Internal Auditor shall also be responsible for retaining the original:
- Authorisation application forms along with any supplementary documentation and notification of the approval given by the authorising officer including a record of the periods over which surveillance took place
 - The magistrate's approval form
 - The frequency of reviews prescribed by the authorising officer and a record of the result of each review of the authorisation
 - Of any renewal forms authorised together with any supporting documentation submitted when the renewal was requested
 - Cancellation forms.
- 4.41 Where the product of surveillance could be relevant to pending or future criminal or civil proceedings it should be retained in accordance with established disclosure requirements.
- 4.42 Generally, all original forms will be retained for at least six years from the date of cancellation. In all cases records will not be destroyed without the authority of the Senior Responsible Officer. Records must be destroyed in accordance with the principles of the Data Protection Act and The Code of Practice.

5. COVERT HUMAN INTELLIGENCE SOURCE (CHIS)

Definition

- 5.1 The Definition of a Covert Human Intelligence Source (CHIS) under the 2000 Act states that a person is a 'CHIS' if:
- (a) They establish or maintain a personal or other relationship with a person for the covert purpose of facilitating the doing of anything falling within paragraph (b) or (c)
 - (b) They covertly use such a relationship to obtain information or to provide access to any information to another person or

(c) They covertly disclose information obtained by the use of such a relationship or as a consequence of the existence of such a relationship

5.2 A relationship is established or maintained for a covert purpose if and only if it is conducted in a manner calculated to ensure that one of the parties to the relationship is unaware of the purpose.

5.3 A relationship is used covertly, and information obtained is disclosed covertly if and only if the relationship is used or the information is disclosed in a manner that is calculated to ensure that one of the parties to the relationship is unaware of the use or disclosure in question.

Risk Assessment - Duty of Care

5.4 When the decision has been taken that the use of 'CHIS' is necessary the Authority has a duty of care to ensure the safety and welfare of the 'CHIS' whilst they carry out the designated actions or tasks.

5.6 Before any action is taken, a full Risk assessment should be undertaken by the Authority to consider all the foreseeable consequences to the CHIS, both during the task, and after the cancellation of the authorisation. Consideration should be given to all appropriate eventualities, including, if the role of the CHIS becomes known. The risk assessment should be updated throughout the tasking to reflect any developments. The ongoing security and welfare of the CHIS should remain a priority.

Authorisation for CHIS

5.7 The conduct or use of a CHIS requires authorisation.

- **Use** of a CHIS is: inducing, asking, or assisting a person to act as a CHIS or to obtain information by means of the conduct of a CHIS
- **Conduct** of a CHIS is: establishing or maintaining a personal or other relationship with a person for the covert purpose of (or incidental to) obtaining, accessing or disclosing information.

5.8 The Council can use CHIS's if, and only if, RIPA procedures are properly followed (see flow chart 2).

5.9 Care must always be taken to ensure that the CHIS is clear on what is/is not authorised at any given time and that all the CHIS's activities are properly risk assessed.

Urgent advice should be sought from an authorising officer should the use and conduct of a CHIS be considered.

5.10 Where a CHIS is used the following records must be kept for each source:

- 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

- 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 the information regarding identity reference 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 s29(5)(a) to (c) of the 2000 Act (Handler and Controller)
- The periods during which those persons have discharged their responsibilities
- The tasks given to the source and the demands made of them in relations to their activities as a source
- All contacts or communications between the source and a person acting on behalf of PCC
- The information obtained by PCC by the conduct or use of the source
- Any dissemination by PCC of information obtained by the conduct or use of the source
- In the case of a source who is not an undercover operative every payment, benefit or reward and offer of payment, benefit or reward that is made or provided by PCC in respect of the source's activities for the benefit of PCC.

5.11 Every source must have a designated Handler and Controller in accordance with s29 (5) (a) to (e) of the RIPA 2000 Act. This states that:

29 (5) For the purposes of this Part there are arrangements for the source's case that satisfy the requirements of this subsection if such arrangements are in force as are necessary for ensuring—

(a) that there will at all times be a person holding an office, rank or position with the relevant investigating authority who will have day-to-day responsibility for dealing with the source on behalf of that authority, and for the source's security and welfare;

(b) that there will at all times be another person holding an office, rank or position with the relevant investigating authority who will have general oversight of the use made of the source;

(c) that there will at all times be a person holding an office, rank or position with the relevant investigating authority who will have responsibility for maintaining a record of the use made of the source;

(d) that the records relating to the source that are maintained by the relevant investigating authority will always contain particulars of all such matters (if any) as may be specified for the purposes of this paragraph in regulations made by the Secretary of State; and

(e) that records maintained by the relevant investigating authority that disclose the identity of the source will not be available to persons except to the extent that there is a need for access to them to be made available to those persons.

Children as Juvenile Sources / Vulnerable adults

- 5.12 Special safeguards apply to the use or conduct of a child juvenile CHIS (a person under 18 years old). An authorisation for the conduct or use of a juvenile source may not be granted or renewed, unless
- (a) an enhanced risk assessment has been undertaken. The risk assessment must demonstrate that,
 - (i) the risk of any type of physical injury and its impact upon the source, which may occur as a result of carrying out the conduct, has been identified and evaluated and
 - (ii) the risk of any psychological distress and its impact upon the source which may occur as a result of carrying out the conduct has been identified and evaluated,
 - (b) the Authorising Officer has considered the risk assessment and is satisfied that any risks identified are justified **and**, that they have been properly explained to and understood by the source and
 - (c) the Authorising Officer knows whether the relationship to which the conduct or use is to relate between the source and a relative, guardian or person who has for the time being assumed responsibility for the source's welfare, and, if it is, has given particular consideration to whether the authorisation is justified in the light of that fact.

On **no** occasion can a child under 16 years of age be authorised to give information against their parents or any person who has parental responsibility for them.

Where a source is under the age of sixteen, an appropriate adult must be present at all meetings which take place between the source and Council investigators. An appropriate adult is,

- (a) The parent or guardian of the source,
- (b) Any other person who for the time being has assumed responsibility for their welfare, or
- (c) If (a) or (b) not available any responsible person aged 18 or over who is neither a member of nor employed by any relevant investigating authority.

The duration of any authorisation is one month from the time of grant or renewal (instead of twelve months), and the authorisation should be subject to frequent reviews.

- 5.13 Special safeguards also apply to the authorisation of a vulnerable adult as a CHIS. A vulnerable adult is a person aged 18 or over who by reason of mental disorder or vulnerability, other disability, age, or illness, is or may be unable to take care of themselves, or unable to protect themselves against significant harm or exploitation. Where it is known or suspected that an adult may be vulnerable, they should only be authorised to act as a CHIS in exceptional circumstances.

- 5.14 A vulnerable adult will only be authorised to act as a source in the most exceptional of circumstances and the authorising officer is satisfied that
- (a) they have considered the results of an appropriate risk assessment,
 - (b) they believe that the risks of harm identified by that risk assessment have been properly explained to and understood by the vulnerable adult source, and
 - (c) they have taken into account the need to safeguard and promote the best interests of the vulnerable adult source.
- 5.15 A juvenile source or vulnerable adult source will only be authorised by the Chief Executive Officer or in their absence the person acting as the Head of Paid Service.

Test Purchases and CHIS's

- 5.16 Carrying out test purchases will not generally require the purchaser to establish a relationship with the supplier with the covert purpose of obtaining information and, therefore, the purchaser will not normally be a CHIS. For example, authorisation would not normally be required for test purchases carried out in the ordinary course of business e.g., walking into a shop and purchasing a product over the counter.
- 5.17 Developing a relationship with a person in the shop, to obtain information about the seller's suppliers of an illegal product e.g., illegally imported products will require authorisation as a CHIS. Similarly, using mobile, hidden recording devices or cameras to record what is going on in the shop will require authorisation as directed surveillance. Note that a CHIS may be authorised to wear a hidden camera without the need for an additional directed surveillance authorisation.

6. CCTV & Aerial Covert Surveillance

CCTV

- 5.1 The use of CCTV must be accompanied by clear signage in order for monitoring to be overt. If it is intended to use CCTV for covert monitoring e.g. by using either hidden cameras or without any signs CCTV is in operation then RIPA authorisation is likely to be required. In any case CCTV must be used in accordance with the Codes of Practice and Protection of Freedoms Act.

Aerial Covert Surveillance

- 6.2 Where surveillance using airborne crafts or devices, for example helicopters or unmanned aircraft (colloquially known as 'drones'), considerations should be made to determine whether a surveillance authorisation is appropriate. In considering whether the surveillance should be regarded as covert, account should be taken of the reduced visibility of a craft or device at altitude. If in doubt please contact an Authorising Officer to seek additional clarity.

7. COMMUNICATIONS DATA

Definition

- 7.1 The Investigatory Powers Act 2016 (IPA) is the legislation governing the acquisition

of Communications Data (CD) by Portsmouth City Council.

Section 60A of the Act provides for the independent authorisation of communications data requests by the Investigatory Powers Commissioner (IPC). The National Anti-Fraud Network (NFN) provides the services of a dedicated SPoC for acquisition of CD (among other functions). The Office for Communications Data Authorisations (OCDA) provides the independent authorisation role on behalf of IPC. An authorising officer in OCDA can authorise any request, for any purpose requested from Portsmouth City Council provided it meets the correct application criteria.

7.2 The IPA has introduced new definitions of categories of Communications Data which replace those previously described within RIPA. The new categories Are Entity Data and Events Data. The definitions are,

- Entity Data relates to the association between an entity and a telecommunications service or telecommunications system and could provide description and identification of an entity. Entity Data is considered to be less intrusive than Events Data. It can be obtained for the prevention and detection of crime.
- Events Data is any data which identifies or describes an event, (whether or not by reference to its location) on, in or by means of a telecommunications system where the event consists of one or more entities engaging in a specific activity at a specific time. Event data can only be obtained for the prevention and detection of SERIOUS crime. Serious Crime is defined as,
 - An offence by a person who is not an individual (i.e. a corporate body)
 - Violence, substantial financial gain, large number of persons in pursuit of a common purpose or person of 18 years with no previous convictions could reasonably be expected to be sentenced to 12 months or more imprisonment.
 - An offence which involves, as an integral part of it, the sending of a communication.
 - An offence which involves, as an integral part of it, a breach of a person's privacy.
 - Internet connection records. – not for local authorities.

7.3 Portsmouth City Council is entitled to acquire entity and event data where criteria apply data **except for** Internet Connection Records.

Examples of entity data are,

- i. Subscriber checks,
- ii. Subscribers or account holders account information,
- iii. Information about the connection, disconnection, and reconnection of services for the subscriber or account holder,
- iv. Information about devices used or available to the subscriber or account holder and,
- v. Information about selection of preferred numbers or discount calls.

Examples of event data are,

- i. information tracing the origin or destination of a communication including incoming call records,
- ii. information identifying the location of apparatus when a communication is, has been or may be made or received.

- iii. information identifying the sender or recipient (including copy recipients) from data in or attached to the communication,
- iv. routing information identifying apparatus through which a communication is or has been transmitted.
- v. itemised telephone call records and timings and duration.
- vi. information about amounts of data downloaded and/or uploaded,
- vii. information about services which the user is allocated or has subscribed to e.g., conference calling, call messaging / waiting / barring.

Accessing Communications Data

- 7.4 Portsmouth City Council use the National Anti-Fraud Network (NAFN) as the SPOC (Single Point of Contact). Applications are approved by the designated person (currently Deputy Chief Internal Auditor or Corporate Strategy Manager). The approved application is sent to NAFN who facilitate the process of obtaining authority by OCDA. NAFN notify PCC of the decision and will liaise with the CD providers to obtain the material.

8. NON-RIPA Surveillance

- 8.1 As a matter of law RIPA does not apply to investigations that do not form part of Portsmouth City Council core functions, but this does not preclude the Council's investigators from using DS or CHIS in such other circumstances. As an example, disciplinary investigations are NON-RIPA activities. The application of RIPA investigatory techniques would normally fail to meet the threshold of being necessary, proportionate, and lawful. However, there may be circumstances where the threshold is reached, e.g., in cases of serious misconduct or criminal activity, particularly matters relating to the Councils' cash assets, and where covert monitoring may be used to gather evidence in a way which would not prejudice a criminal investigation or be prejudicial to the Councils interests (see further the Councils Code of Conduct and Communications & Information Systems Use policies)
- 8.2 It is the policy of this Council that, in so far as the law allows, the covert techniques covered by this policy shall **NOT** be undertaken unless authorised in accordance with RIPA. There will be circumstances where covert techniques are required but (normally due to the investigation being into ordinary functions of the Council) they may not be authorised under RIPA. In order to ensure proper adherence to human rights principles in all investigations, it is the policy of this Council to apply RIPA principles to NON-RIPA investigations. In the event that an investigation into a non-core function requires the use of these techniques, the investigator must apply in the same way, using the same forms, to the same Authorising Officer, endorsing the forms clearly in red ink, "NON-RIPA". Where disciplinary matters are concerned, the advice of Human Resources should also be sought. (It should be noted that such NON-RIPA activities would be undertaken at the Council's own risk, as they are not afforded the legal protection provided by RIPA. In any case of doubt as to how NON-RIPA activities should be conducted, the Council's RIPA Monitoring Officer should be contacted for advice and assistance). Portsmouth City Council shall ensure that officers with responsibility for authorising or carrying out surveillance or accessing communications data are aware of their obligations to comply with RIPA and with this policy and any associated procedures. Furthermore, officers shall receive appropriate training and/or be appropriately supervised in order to carry out functions under RIPA. All those involved in the type of activities covered by this

policy (especially Authorising Officers) are instructed to bring any suggestions for continuous improvement of this policy to the attention of the RIPA Coordinator.

9 Record keeping and error reporting.

9.1 Portsmouth City Council should have centrally retrievable records of authorisations for a minimum period of three years from the end of each authorisation (Portsmouth City Council's retention policy for documents is 6yrs as per 4.42 above). The information held within the centrally retrievable records should be regularly updated and made available to the IPC and IPT upon request.

9.2 An error must be reported if it is a "relevant error" to the IPC as soon as reasonably practicable and no later than ten working days after its identification. A relevant error is where the Council errs in complying with requirements imposed by RIPA or IPA. If the IPC considers that the error is a serious error and that it is in the public interest to do so, they will inform the subject of that error.

10 Product Management Processes.

10.1 The Council will ensure that the handling of private information obtained by Covert surveillance or CHIS authorisation comply with relevant legal frameworks, so that any interference with the right to private and family life is justified in accordance with Article 8(2) ECHR.

Use of material as evidence.

10.2 Subject to provisions in the Codes of Practice material obtained through directed surveillance, CHIS, or acquisition of CD may be used as evidence in criminal proceedings. Ensuring the continuity and integrity of evidence is critical. The Council should be able to demonstrate how the evidence has been obtained and managed to the extent required by the relevant rules of evidence and disclosure.

10.3 All material obtained through a RIPA / IPA authorisation must be handled in accordance with safeguards aligned to the requirements of the Code of Practice. These safeguards should be made available to the IPC. Breaches of these safeguards must be reported to the IPC in a fashion agreed with him or her. Any personal data breaches should also be reported to the Information Commissioner in accordance with the requirements of the applicable data protection regime.

10.4 Dissemination, copying and retention of material obtained through a RIPA / IPA authorisation must be limited to the minimum necessary for the authorised purposes which are that it is,

- Or is likely to become, necessary for any of the statutory purposes set out in the RIPA 2000 in relation to covert surveillance or authorisation of a CHIS,
- Necessary to do so for facilitating the carrying out of the functions of Portsmouth City Council,
- Necessary to do so for facilitating the functions of the Judicial Commissioners or the Investigatory Powers Tribunal,
- Necessary to do so for the purposes of legal proceedings,
- Necessary to do so to fulfil the functions of any person by or under any enactment.

Storage

10.5 Material obtained through RIPA, IPA or acquisition of CD and all copies, extracts and summaries of it, must be handled and stored securely to minimise the risk of loss or theft. It must be inaccessible to people without the required level of security clearance. This requirement applies to all those who are responsible for the handling of the material.

In particular, the Council must apply the following protective security measures,

- physical security to protect any premises where the information may be stored or accessed,
- IT security to minimise the risk of unauthorised access to IT systems,
- an appropriate security clearance regime for personnel.

Destruction

10.6 Information obtained through RIPA, IPA or acquisition of CD, and all copies, extracts, and summaries which contain such material, should be scheduled for deletion or destruction and securely destroyed as soon as they are no longer needed for the authorised purpose. If such information is retained, it should be reviewed at appropriate intervals to confirm that the justification for its retention is still valid.

Confidential personal information, privileged material and confidential constituent information.

10.7 Particular consideration should be given in cases where the subject of the investigation or operation might reasonably assume a high degree of confidentiality. This includes where the material contains information that is legally privileged, confidential journalistic material or where material identifies a journalist's source, where material contains confidential personal information or communications between a Member of Parliament and another person on constituency business. Separate guidance on each of these categories is available in the relevant Code of Practice and should be referred to as and when required.

Oversight.

10.8 The IPC, and those that work under their authority, will ensure compliance with the law by inspecting public authorities and investigating any issue which they believe warrants further independent scrutiny. The IPC will have unfettered access to all locations, documentation and information systems as necessary to carry out their full functions and duties. Council employees using investigatory powers must provide all necessary assistance to the IPC or relevant representative.

10.9 The Investigatory Powers Tribunal (IPT) has jurisdiction to investigate and determine complaints against the Council's use of investigatory powers.

11 IMPACT RISK ASSESSMENTS

11.1 When considering whether to carry out surveillance it is recommended that an 'impact risk assessment' is carried out and recorded to establish if the proposed course of action is a proportionate response to the problem it seeks to address. An impact risk assessment should be carried out on all activities including those that will not require RIPA authorisation.

11.2 The impact risk assessment involves;

- Identifying clearly the **purpose(s)** behind the monitoring arrangements and the benefits it is likely to deliver.
- Identifying any likely **adverse impact** of the monitoring arrangement
- Considering **alternatives** to monitoring or different ways in which it might be carried out
- Taking into account the **obligations** that arise from monitoring (especially on collateral intrusion)
- Judging whether the monitoring is **justified**

11.3 Adverse Impact- consideration should be given to:

- What intrusion, if any will there be into the private lives of workers and others, or interference with their private activities, emails, telephone calls or other correspondence.
- Whether those who do not have a business need to know will see information that is confidential, private or otherwise sensitive.
- In the case of surveillance on an employee, what impact, if any, will there be on the relationship of mutual trust and confidence that should exist between workers and their employer?

11.4 Alternatives – questions that should be asked:

- Are there other methods of obtaining the required evidence/information without carrying out covert surveillance, e.g. intelligence gathered from elsewhere.
- Has consideration been given to writing to the individual(s) informing them of the issue and advising that monitoring will be carried out over a specified period? (remember collateral intrusion could still apply to their colleagues or family etc)
- Has consideration been given to carrying out overt surveillance as part of officers' normal duties?
- Can established or new methods of supervision, effective training and or clear communication from managers, rather than electronic or other systemic monitoring, deliver acceptable results?
- Can monitoring be limited to those individuals and workers about whom complaints have been received, or about whom there are other grounds to suspect of wrongdoing?
- Can monitoring be automated? If so, will it be less intrusive, e.g. does it mean that private information will be 'seen' only by a machine rather than by other workers?
- Can spot-checks be undertaken instead of using continuous monitoring?

11.5 Obligations – means considering the following:

- Whether and how individuals or employees will be notified about the monitoring arrangements.
- How information about the individual or employee collected through monitoring will be kept securely and handled in accordance with the Act and

DPA requirements.

- The implications of the rights that individuals have to obtain a copy of information about them that has been collected through monitoring.

11.6 Justified – involves considering:

- The benefit of the method of monitoring/surveillance
- Any alternative method of monitoring/surveillance
- Weighing these benefits against any adverse impact
- Placing particular emphasis on the need to be fair to the individual worker or person
- Ensuring, particularly where monitoring electronic communications of employees' is involved, that any intrusion is no more than absolutely necessary

12. FURTHER GUIDANCE

12.1 Guidance is provided as a reminder of the authorisation process (the Magisterial approval process is in addition to these) and can be located as appendices to this document

[Flowchart 1: Surveillance, guidance.](#)

[Flowchart 2: CHIS guidance.](#)

[Flowchart 3: Accessing communications data](#)

[Surveillance an aid to investigation Guidance](#)

12.2 Appendix A of this document provides the relevant contact details of the officers who may authorise surveillance, the use of a CHIS and give advice on accessing communications data.

13 OVERSIGHT AND IPCO GUIDANCE

Senior Responsible Officer

13.1 The Senior Responsible Officer (currently at Portsmouth City Council – Elizabeth Goodwin - Chief Internal Auditor) must review each authorised RIPA to ensure that they are being authorised in accordance with the Code and to identify any training requirements.

13.2 Requests for guidance from The Investigatory Powers Commissioner's Office (IPCO) must only originate from the Senior Responsible Officer. The IPCO has made it clear that it does not give legal advice and any opinion given in a reply to a request for guidance does not constitute legal advice and should not be cited as the definitive advice of the IPCO.

Members

13.3 The RIPA Policy must be reviewed when there are any changes in personnel, legislation or codes of practice and any amendments must be approved by the Governance and Audit and Standards Committee.

13.4 Regular reports of Authorised applications must be submitted to the Governance

and Audit and Standards Committee by the Senior Responsible Officer along with an opinion on any training requirements or where the Code has not been followed.

Investigatory Powers Commissioners Office

- 13.5 The Investigatory Powers Commissioner's Office provides independent oversight of the use of the powers contained within the Regulation of Investigatory Powers 2000. This oversight includes inspection visits by Inspectors appointed by the IPCO.

14 COMPLAINTS

The Regulation of Investigatory Powers Act 2000, (the UK Act), establishes an independent Tribunal. This has full powers to investigate and decide any cases within its jurisdiction. Details of the relevant complaints procedure can be obtained from:

Investigatory Powers Tribunal
PO Box 33220
London
SW1H 9ZQ - Tel: 020703537111

Appendix A

CONTACTS

Authorising Officers:

RIPA & Approved Ranked Officer

Paul Somerset, Deputy Chief Internal Auditor

paul.somerset@portsmouthcc.gov.uk

Tel: 023 9283 4673

RIPA & Approved Ranked Officer

Paddy May, Corporate Strategy Manager

paddy.may@portsmouthcc.gov.uk

Tel: 023 9283 4020

Senior Responsible Officer:

Elizabeth Goodwin, Chief Internal Auditor

elizabeth.goodwin@portsmouthcc.gov.uk

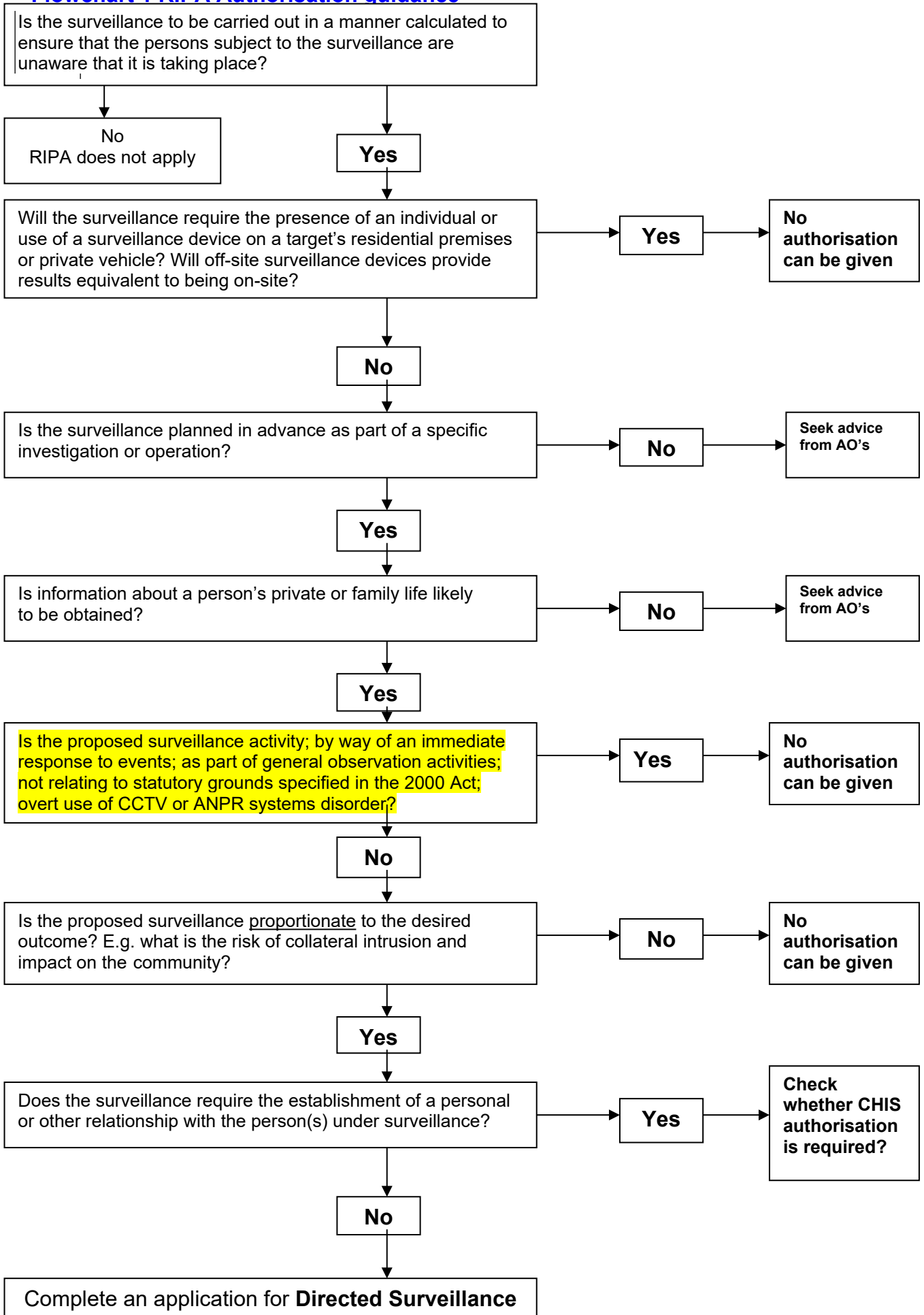
Tel: 023 9283 4682

Monitoring Officer:

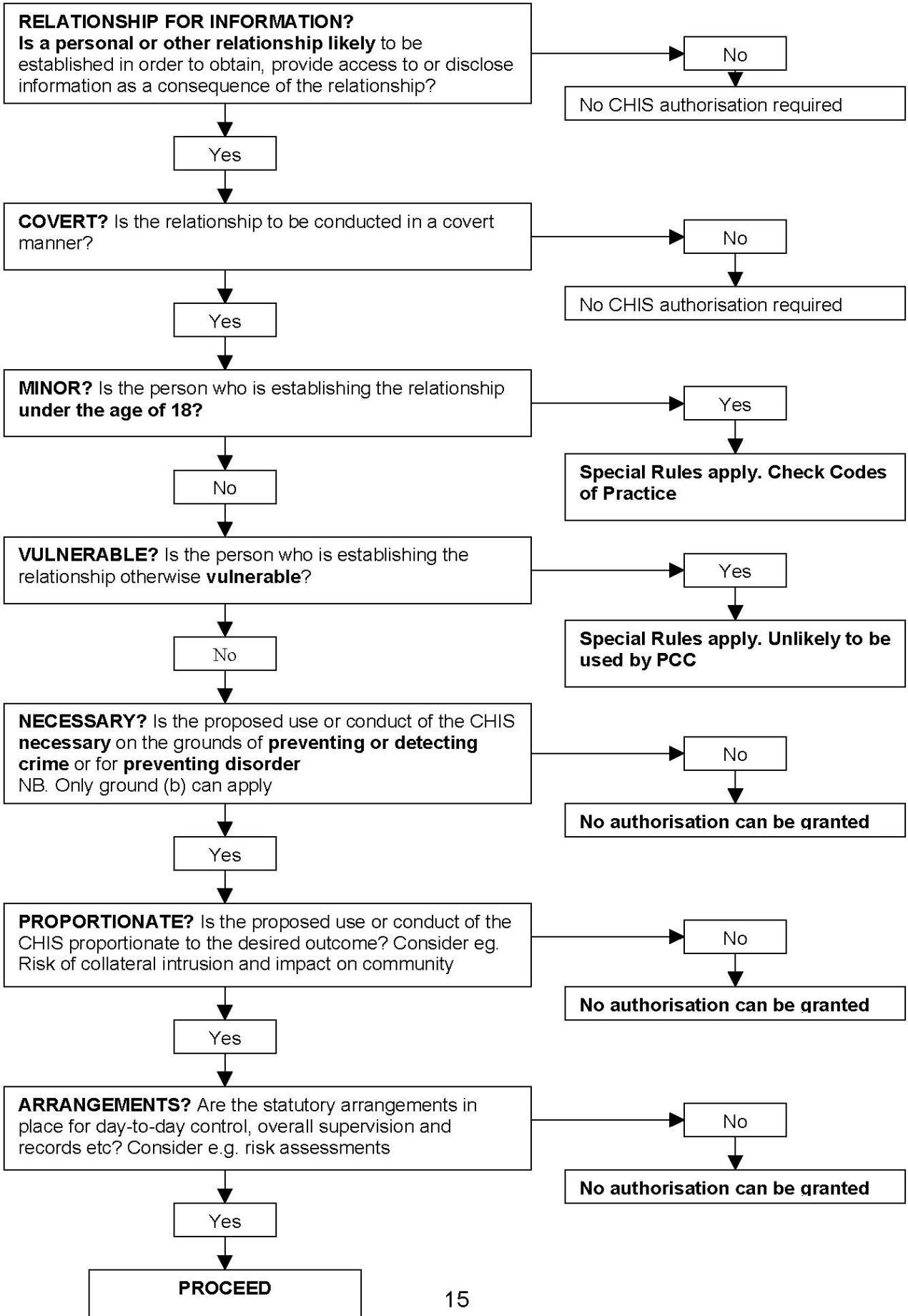
Peter Baulf, City Solicitor & Monitoring Officer

Peter.baulf@portsmouthcc.gov.uk

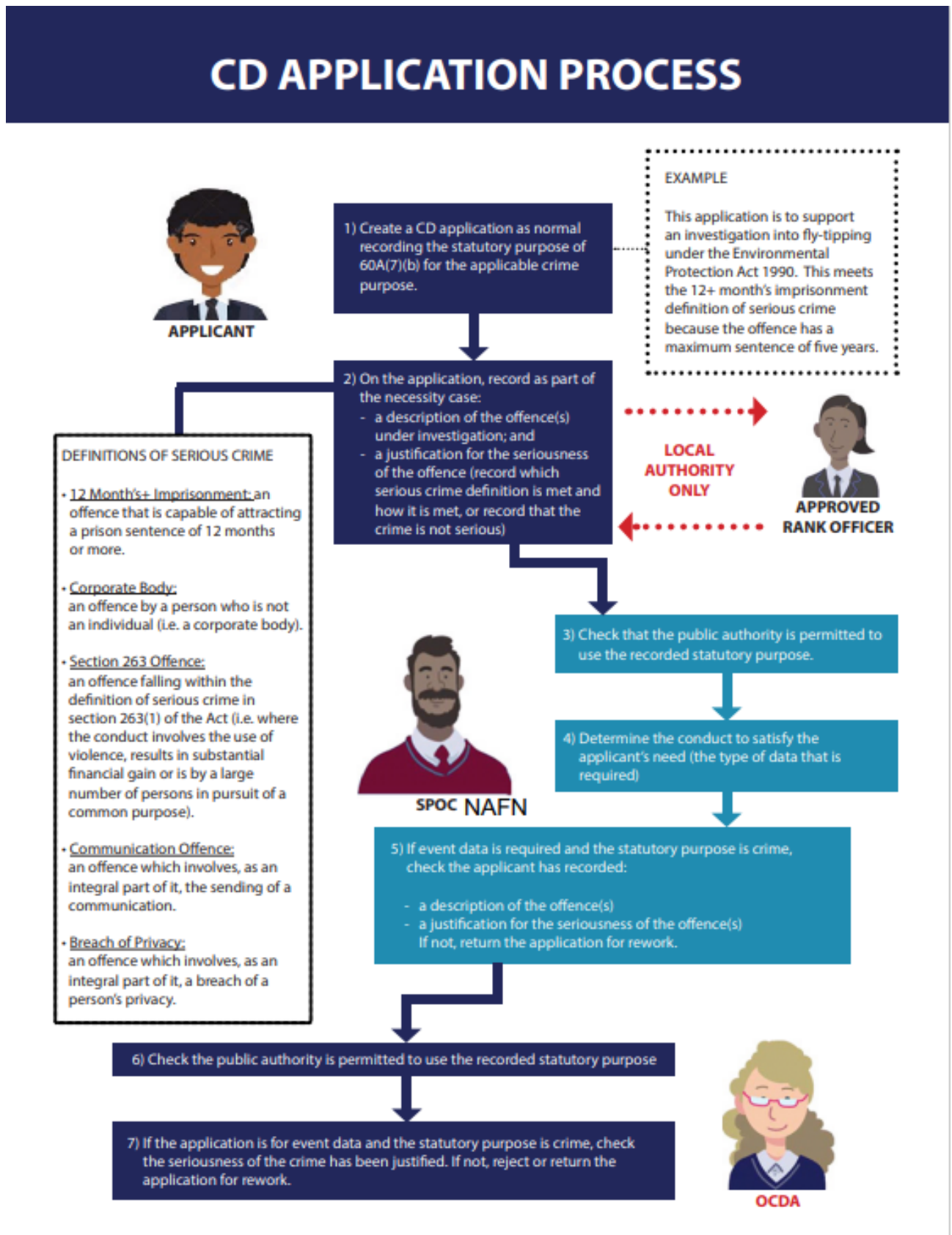
Flowchart 1 RIPA Authorisation guidance



Flowchart 2 – CHIS Guidance



Flowchart 3 – Accessing Communications Data



Note: If at any time during the process, the data is no longer required for any reason. The SPOC officer should be informed and the Designated Person will complete the relevant cancellation notice (ACD819) which is forwarded to the Data service Provider

Impact Risk Assessment Form

Date and Time:
Name and Title:
Details of the operation / investigation
Details of the offence(s) / Breach(s)
Proposed actions
Purpose of the proposed actions and benefits it is likely to deliver
Identify any likely adverse impact of these actions
Are there any alternatives i.e., different ways in which the desired outcome could be achieved?

Are there any obligations that arise from the proposed actions?

How are these actions justified?

Does RIPA need to be considered?

Signature

Date and Time

SURVEILLANCE - AN AID TO INVESTIGATION

DEFINITION

1. Surveillance is the continuous watching (overt or covert) of persons, vehicles, places or objects to obtain information concerning the activities and identities of individuals.

OBJECTIVES OF SURVEILLANCE

2. Surveillance operations can have some of the following objectives:
 - a. To obtain evidence of a crime.
 - b. To locate persons by watching their haunts and associates.
 - c. To obtain detailed information about a subject's activities.
 - d. To check on the reliability of informants.
 - e. To obtain information for search warrants*.
 - f. To prevent an offence or to *arrest a subject in commission of an offence.
 - g. To obtain information for later use in an interview.
 - h. To develop leads and information received from other sources.
 - i. To know at all times the whereabouts of an individual.
 - j. To obtain evidence for use in court.

TYPES OF SURVEILLANCE

3. The following types of surveillance can be carried out:
 - a. Covert Surveillance
A secretive watch where the subject is not aware of our presence.
 - b. Overt Surveillance
An open observation where we deliberately expose the operatives to a subject. (Used as a deterrent).
 - c. Static Surveillance
The use of a vehicle, building or street furniture (for a short time only) as an observation post (OP) from which to observe a subject or premises or to act as the "trigger" for foot or mobile surveillance.
 - d. Mobile Surveillance
The use of cars to follow a subject who is travelling by vehicle. Motorcycles can be used as part of a mobile surveillance operation.

e. Technical Surveillance*

The use of technical equipment such as "bugs" to monitor the activities of a subject(s). This is a very specialised skill. ***not applicable n.b. Portsmouth City Council do not have the legal powers to do this**

The neumonic ADVOKATE is a useful aid to ensure that any information gained by carrying out surveillance will stand up to cross-examination in court.

- A** Amount of time
How long was the subject actually in view?

- D** Distance
How far away from you was the subject?
Did you have to use binoculars?
Did you have to avoid the subject's gaze?

- V** Visibility
What is your vision like?
Do you have to wear glasses - and were you wearing them at the time?
Were you looking through a windscreen or into a vehicle mirror?
Were the mirrors misted up?
What was the weather like - foggy; where was the sun?

- O** Obstacles
Were there any obstacles to your vision - bushes, cars, people?

- K** Known
Is the subject known to you?
If so, how?
If not - how did you recognise the subject?

- A** Any reason to remember the subject?
Brightly coloured or unusual clothes.
Looked like a famous person.

- T** Time
How long after seeing the subject did you make notes?
Could you have forgotten or confused anything since you last saw the subject?

- E** Errors
Could you have made a mistake in identifying the subject?
If not, why not?

DESCRIPTION OF PEOPLE

- A** Age
Approximate within 4 years, ie 20-24

- B** Build
Qualify by example if possible

- C** Clothing
Uniforms, brands, logos, etc

- D** Distinguishing Marks
Tattoos, scars, complexion

- E** Elevation/Height
Approximate within 4", ie, 5`2 - 5`6

- F** Face
Complexion, facial hair, glasses, jewellery

- G** Gait
How they walk

- H** Hair
Style, colour, length, etc

DESCRIPTION OF VEHICLE

- S** Shape
Saloon, estate, mpv, etc

- C** Colour
Basic/metallic

- R** Registration
Full/part

- I** Identifying Marks
Dents, alloy wheels, lights, etc

- M** Make and Model

PRE-SURVEILLANCE CHECKLIST

Before carrying out a surveillance operation the following factors need to be checked by a ground reconnaissance or, if this is not possible, a map study.

DO YOU REALLY NEED TO CARRY OUT SURVEILLANCE - CAN YOU OBTAIN THE NECESSARY INFORMATION BY OTHER MEANS?

IF NOT, SOME OF THE THINGS TO CONSIDER FIRST BEFORE DEPLOYING....

ROUTES IN AND OUT

LIKELY DROP OF POINTS (DOPs)

BEST APPROACHES

FROM WHERE CAN YOU SEE THE TARGET CLEARLY?

CAN ALL APPROACHES/EXITS BE SEEN?

CAN YOU BE OBSERVED OR OVERLOOKED?

WILL YOU BE OBVIOUS?

WHERE CAN ANY BACK-UP BE LOCATED?

ARE COMMUNICATIONS REQUIRED?

DO ALL COMMUNICATIONS WORK?

IS AN EMERGENCY RV REQUIRED - IF SO, WHERE WILL IT BE LOCATED?

ARE ANY SPECIAL PREPARATIONS REQUIRED?

IS THERE ANY SPECIAL EQUIPMENT REQUIRED?

WHERE ARE THE MOST APPROPRIATE REST AREAS, FOOD SOURCES, TOILETS ETC?


A GUIDE TO PREPARATION AND USE OF SURVEILLANCE LOGS

1. Surveillance logs constitute original notes of evidence and as far as practicable it is essential that they are prepared and preserved strictly in accordance with rules of evidence, ie, where items have been deleted they must be initialed by the person making the entry. Each entry must follow consecutively with no spaces left.
2. Where a dedicated loggist is appointed, it is his/her responsibility to accurately record events as they are transmitted or reported to him/her.
3. The loggist will be responsible for completing daily, at the commencement of the surveillance, details of the persons employed. These details will be recorded on the opening page.
4. The loggist will record the date, time, his/her name and the fact he/she is performing the duty of loggist. On being relieved, regardless of the length of absence, he/she will "sign off" adopting the same procedure as that when signing on. When it is not practical to conform strictly to these procedures, eg, where the loggist has to leave his/her vehicle in order to participate in the surveillance, such facts should be recorded as soon as practicable.
5. The person who witnesses a particular event will, if it is not his/her own entry, initial alongside the entry where his/her name appears at the first available opportunity. He/she must also sign and date the log at the conclusion of the notes. In the cases where a dedicated loggist is not appointed or where it is not possible to communicate with the loggist, the person witnessing must record details of the event at the time or as soon as practicable.
6. Where notes are not made at the time of the occurrence they must be made as soon as practicable. Notes will be followed by the date, time and place the notes are made.
7. Where two or more persons are present at an occurrence, there is no objection to them collaborating when preparing their notes so that the notes may be as full and comprehensive as possible. Where notes have been made by only one person, there is no objection to these notes being used by another person when giving evidence, provided the person who has not written the notes, reads them as soon as possible after they are made, accepts that they are accurate, and signs and dates them. A note whether made in collaboration with a colleague or otherwise, or if made by a colleague, must only reflect the person's genuine personal observation and recollection.
8. The taking of original notes is of the utmost importance because the notes may later have to be produced in court or referred to by the person long after they were made.
9. The general preference is that the 24 hour clock is used in the log book.
10. No erasure or obliteration of notes is permissible at any time and once an entry in a book has been signed, it cannot be altered in way, either by adding, deleting or changing any particulars. Any corrections made before presentation are to be initialed. If additional or corrected information is obtained subsequently, a further and separate entry is to be made.
11. The pages of the log book are to be numbered. A page-numbered book should be used for this purpose. No pages may be removed. At the conclusion of the operation, the log book should be stored with the remainder of the papers for future production as required.

12. Unnecessary spaces will be avoided between words or at the end of lines. Unused spaces should be struck out and, if a space is left after recording, a line drawn to the end and initialed.
13. Overwriting is forbidden. If a mistake is made, eg, if a wrong word is used or if a word is mis-spelt, it must be struck out and initialed and the letter "A" inserted. At the foot of the page, before it is signed, the letter "A" is again to be inserted followed by the correction. If a second or third mistake is found, the letter "B" and "C" are to be used as necessary. If there is no room at the foot of the page, the corrections may be added at the end of the log for the day.
14. The log book should be available for production if required by the court, or Counsel who desire to examine them. Copies of notes must not be taken to Court; the original must be used in every case. If it should be necessary to make an original note on a loose piece of paper and subsequently copy it into the log book, the original note must be carefully preserved for production if required.

REMEMBER!

In the event of criminal proceedings taking place against a subject, a poorly maintained or inaccurate surveillance log can result in a case being dismissed with many, many hours of wasted effort.



**PART II OF THE REGULATION OF INVESTIGATORY
POWERS ACT (RIPA) 2000
APPLICATION FOR AUTHORISATION TO CARRY OUT
DIRECTED SURVEILLANCE**

<https://www.gov.uk/government/publications/application-for-use-of-directed-surveillance>

**PART II OF THE REGULATION OF INVESTIGATORY
POWERS ACT (RIPA) 2000
REVIEW OF A DIRECTED SURVEILLANCE AUTHORISATION**

<https://www.gov.uk/government/publications/review-of-use-of-directed-surveillance>

**PART II OF THE REGULATION OF INVESTIGATORY
POWERS ACT (RIPA) 2000
CANCELLATION OF A DIRECTED
SURVEILLANCE AUTHORISATION**

<https://www.gov.uk/government/publications/cancellation-of-use-of-directed-surveillance-form>

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

Local authority:.....

Local authority department:.....

Offence under investigation:.....

Address of premises or identity of subject:.....

.....

.....

Covert technique requested: (tick one and specify details)

Communications Data

Covert Human Intelligence Source

Directed Surveillance

Summary of details

.....

.....

.....

.....

.....

.....

Note: this application should be read in conjunction with the attached RIPA authorisation/RIPA application or notice.

Investigating Officer:.....

Authorising Officer/Designated Person:.....

Officer(s) appearing before JP:.....

Address of applicant department:.....

.....

Contact telephone number:.....

Contact email address (optional):.....

Local authority reference:.....

Number of pages:.....

Order made on an application for judicial approval for authorisation to obtain or disclose communications data, to use a covert human intelligence source or to conduct directed surveillance. Regulation of Investigatory Powers Act 2000 sections 23A, 23B, 32A, 32B.

Magistrates' court:.....

Having considered the application, I (tick one):

- am satisfied that there are reasonable grounds for believing that the requirements of the Act were satisfied and remain satisfied, and that the relevant conditions are satisfied and I therefore approve the grant or renewal of the authorisation/notice.
- refuse to approve the grant or renewal of the authorisation/notice.
- refuse to approve the grant or renewal and quash the authorisation/notice.

Notes

.....

.....

.....

.....

.....

Reasons

.....

.....

.....

.....

.....

.....

Signed:

Date:

Time:

Full name:

Address of magistrates' court: