Portsmouth CITY COUNCIL

Agenda item:

Decision maker:	Governance & Audit & Standards Committee
Subject:	Regulation of Investigatory Powers Act 2000 (RIPA)
Date of decision:	14th March 2013
Report from:	Michael Lawther City Solicitor and Strategic Director
Report by:	Lyn Graham, Chief Internal Auditor
Wards affected	All
Key decision (over £250k)	N/A

---

1. Summary

1.1 One Regulation of Investigatory Powers Act (RIPA) application has been made since the last report to Governance and Audit Members in November 2012 regarding communications data. There have been some slight amendments required to Policy and the changes have been provided to all relevant staff. We have been notified that the Office of Surveillance Commissioners (OSC) will inspect our RIPA records on the 4th April 2013.

2. Purpose of report

2.1 To update Members on the Authority's use of Regulatory Powers for the five month period from November 2012 to March 2013 and the changes required to Policy; to advise on training provided and the impending visit by the OSC Inspector.

3. Background

3.1 PCC has a policy and procedures to ensure that officers comply with the Regulation of Investigatory Powers Act requirements to mitigate any legal challenge risks and this is updated when there are changes in the codes of practice or legislation including case law.

3.2 To ensure continuing compliance with the Codes of Practice training on RIPA is provided to relevant officers annually.

3.3 The Authority is subject to inspection usually every two years but sometimes longer by the Office of Surveillance Commissioners (OSC) and was last inspected by them in April 2010 and the findings reported to this Committee.

4. Recommendations

It is recommended that Members of the Governance and Audit and Standards Committee:

4.1 Note the RIPA application authorised in the five month period from November 2012 to March 2013,

4.2 Approve the required changes to Policy,

4.3 Note the OSC inspection due on the 4th April 2013,

4.4 Note that update training has been provided to relevant officers.

5. Regulation of Investigatory Powers Act Authorisations

5.1 Currently the Authority uses the National Anti Fraud Network (NAFN) as a Single Point of Contact (SPOC) to authorise communications data applications on our behalf. However under the new Protection of Freedoms Act the Council still has to take the authorised RIPA's for communications data to the Magistrate for Judicial approval.

5.1 One RIPA application for communications data has been authorised in the five month period between November 2012 and March 2013 to assist with an investigation into the sale of counterfeit goods via a website. The application was authorised by NAFN and taken to Magistrates by the investigating officer and approval obtained.

6. Training

6.1 The three authorising officers received training in the new procedures involving magisterial approval on October 31st 2012 and 20 officers from enforcement, licensing, counter fraud and trading standards received training on the 10th January 2013.

7. Changes to Policy

7.2 The proposed changes to the RIPA Policy are highlighted in the attached Policy (Appendix A). These were provisionally approved by the Chair of this Committee on the 14th January to enable relevant officers to receive an up to date copy of the Policy as soon as possible to assist them in their duties, with the understanding that it would be brought to the next meeting of this Committee for full approval.

7.3 Changes mainly relate to test purchases, drive bys and the process for magisterial approval.

8. Equality impact assessment (EIA)

This is an information report only and therefore does not require an equalities impact assessment. The RIPA Policy is subject to an equalities assessment.

9. City Solicitor's comments

The Legal implications are incorporated within the body of this report. There are no other immediate legal implications arising from this report

10. Head of Finance's comments

N/A

……
Signed by: Michael Lawther, City Solicitor and Strategic Director

Appendices: Appendix A RIPA Policy and Procedures minus forms and flowcharts

Background list of documents: Section 100D of the Local Government Act 1972
The following documents disclose facts or matters, which have been relied upon to a material extent by the author in preparing this report:

Title of document		**Location**
1	Covert Surveillance Code of Practice Issued by the Home Office and Covert Human Intelligence sources Code of Practice issued by the Home Office	http://www.homeoffice.gov.uk/counter-terrorism/regulation-investigatory-powers/Regulation of Investigatory Powers Act-codes-of-practice/
2	Regulation of Investigatory Powers Act 2000	http://www.legislation.gov.uk/ukpga/2000/23/contents
3	Portsmouth City Council Regulation of Investigatory Powers Act Policy	http://intralink/Media/Revised_RIPA_Policy.pdf
4	Home Office guidance	http://www.homeoffice.gov.uk/publications/counter-terrorism/ripa-forms/local-authority-ripa-guidance/?view=Standard&pubID=1079688
5	Protection of Freedoms Bill	http://www.homeoffice.gov.uk/publications/about-us/legislation/protection-freedoms-bill/

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

ID	*Counter Fraud -RIPA*
Last Review Date	*January 2013*
Next Review Date	*January 2014*
Approval	*Governance and Audit and Standards Committee.*
Policy Owner	*Michael Lawther Strategic Director and Monitoring Officer also Senior Responsible Officer for RIPA*
Policy Author	*Lyn Graham Chief Internal Auditor*
Advice & Guidance	Lyn Graham, Tel: 023 9283 4668 Chief Internal Auditor lyn.graham@portsmouthcc.gov.uk
Location	*Intralink*
Related Documents	Covert Surveillance Code of Practice; Regulation of Investigatory Powers Act 2000; Protection of Freedoms Bill
Applicability	*All PCC Staff*

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) and RIPA (Directed Surveillance and Covert Human Intelligence Sources) Order 2010 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 and detection of crime.

3. The Protection of Freedoms Act 2012 requires that RIPA is only used for criminal offences that could attract a custodial sentence of 6 months or more, or relate to tobacco or alcohol sales to children. Applications once authorised have to be approved by a Magistrate.

4. RIPA controls the use of various methods of investigation, in particular the use of covert surveillance, covert human intelligence sources (CHIS) and accessing communication data and defines what constitute these activities.

5. If the activities proposed by investigating officers fall within the definitions (see Section 3) then this Policy, Procedures and the 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)

6. 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 surveillance, it becomes directed surveillance and requires a RIPA authorisation.

7. All directed surveillance, using a CHIS or accessing communications data must be properly authorised. Failure to secure proper authorisation and 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 Office of the Surveillance Commissioner 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
7. Communications Data
8. Impact Risk Assessment
9. Further Guidance
10. Oversight
11. Complaints

Appendix A: List of Authorised Persons
Flowchart 1: Surveillance, guidance.
Flowchart 2: CHIS guidance.
Flowchart 3: Accessing communications data
Flowchart 4: Duration of authorisation and renewals
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/

http://www.homeoffice.gov.uk/publications/counter-terrorism/ripa-forms/local-authority-ripa-guidance/?view=Standard&pubID=1079688

1. Policy Statement

1.1 In some circumstances, it may be necessary for Portsmouth City Council employees, 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 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 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 where it is necessary for the "prevention or detection of crime or disorder" and where it has been demonstrated to be necessary and proportionate in what it seeks to achieve and meets home office requirements.

1.6 This policy makes a number of references to confidential information. The Revised Code of Practice which came into effect on the 6th April 2010 requires the highest levels of authorisation where 'confidential information' is likely to be acquired and at PCC this is the Chief Executive. [Refer to Definitions in Section 3]

1.7 The Authority will make arrangements to ensure that the Code of Practice is complied with including having Member and Senior Officer oversight to ensure that The Code is complied with and appropriate training is given to officers.

1.8 Statutory Instrument 2003 No 3171 restricts authorising officers in local authorities to prescribed offices of no lower a level than assistant chief officer, assistant 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 Protection of Freedoms Act 2012 and the Code of Practice on Covert

Surveillance and the Code of Practice on the Use of Covert Human Intelligence Sources.

3. TERMS EXPLAINED

3.1 **Authorising officer** is the person(s) who is entitled to give an authorisation for directed surveillance in accordance with the Regulation of Investigatory Powers Act 2000 and The Code of Practice.

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 informer, volunteer or Council officer in striking up a relationship with someone as part of an investigation to obtain information "under cover".

Someone who volunteers information to the 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 use of a CHIS. However, relying on an individual to ask questions with a view to gathering evidence, may amount to use of a CHIS.

3.3 **Collateral Intrusion** means the obtaining of private information about the subject of the covert surveillance whether or not that person is specifically targeted for purposes of the investigation and could include their families, colleagues, friend or associates amongst others. 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.

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.

Similarly, although overt, town-centre CCTV cameras do not normally require authorisation. If, however the camera is tasked for a specific purpose, which involves prolonged surveillance on a particular person, authorisation must be obtained.

3.4 **Confidential Material** Confidential information consists of matters subject to legal privilege, confidential personal information or confidential journalistic material. 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.

3.5 **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.

3.6 **Directed surveillance** is surveillance which is:-

- Covert;

- Not intrusive surveillance (see definition below - Portsmouth City Council must not carry out any intrusive surveillance);
- Not carried out as an immediate response to events which would otherwise make seeking authorisation under the Act not reasonably practicable (e.g. spotting something suspicious and continuing to observe it as part of business as usual) and
- Is undertaken for the purpose of a specific investigation or operation in a manner likely to obtain private information about a person (whether or not that person is specifically targeted for purposes of the investigation) and is for the sole purpose of preventing or detecting crime.
- ***All directed surveillance must be RIPA authorised.***

(Please note - "private information" in relation to a person includes any information relating to their private or family life, their home and their correspondence.)

3.7 **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 local authorities.

3.8 **Necessity** means that there is no reasonable and effective alternative way of achieving the desired objective(s).

3.9 **Overt (or 'open') surveillance.** Surveillance will be overt if the subject has been told that it will happen. N.b. you do have to be careful however about obtaining private information on others that have not been informed
Overt
• Police Officer, Street Warden, Enforcement Officer or Ranger on routine patrol
• Sign-posted Town Centre 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.
• Most test purchases 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).
Overt but not requiring prior authorisation
• CCTV cameras providing general traffic crime or public safety information

3.10 **Private information** includes information about a person relating to his/her private or family life.

3.11 **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.

3.12 **Proportionality** means that the use of surveillance is not excessive, i.e. that it is in proportion to the significance and level of offence being investigated and collateral intrusion impacts.

3.13 **Residential premises** means any premises occupied or used, however temporarily, for residential purposes or otherwise as living accommodation.

3.14 **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; and 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 LACORS guidance 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 maybe construed as covert surveillance and an impact assessment/ RIPA authorisation maybe required.

Drive Bys

4.5 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.

Employee Investigations

4.6 For employment investigations of non criminal activity if covert surveillance is proposed 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

4.7 Applications where a significant risk of acquiring confidential material has been identified 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.

4.8 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

Juvenile or vulnerable Individual CHIS's

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

Authorisation Procedure

4.10 Applications for directed surveillance will be authorised by either the Chief Internal Auditor or the Deputy Chief Internal Auditor or the Corporate Strategy Manager.

4.11 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.

4.12 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.

4.13 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 for that RIPA once approved by a Magistrate. It will be the Investigating Officer's responsibility to submit the application to the Magistrate following authorisation to do so from the City Solicitor to represent the Council, as required under Section 223 of the Local Government Act. The investigating Officer must ensure that all staff involved with the investigation understands what has been authorised and approved and they must all sign the forms to that effect.

4.14 All requests to Magistrates will be on the forms as provided in the Code of Practice issued by the OSC.

4.15 All applications for directed surveillance renewals will be made on the official form. 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.

4.16 Where authorisation ceases to be either necessary or appropriate the authorising officer will cancel an authorisation using the official form.

4.17 Further guidance can be obtained from the Office of Surveillance Commissioners including the Codes of Practice: http://www.surveillancecommissioners.gov.uk/advice_ripa.html

4.18 Any person giving an authorisation for the use of directed surveillance must be satisfied (believe) 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
- specific targeted criminal offence that carries a maximum sentence of 6 months or more imprisonment, or is one of the exemptions

Urgent Cases

4.19 Cases will not normally be regarded as urgent unless the time that would elapse before the authorising officer is available to grant authorisation would in the judgement of the authoriser be likely to endanger life or jeopardise the operation or investigation. In practice these should be few and far between. In urgent cases the authorising officer may give an oral authorisation (which must have the approval of a Magistrate). A statement that the authorising officer has expressly granted the authorisation should be recorded on the

form, or, if that is not possible, in the applicant's notebook or diary. This should be done by the person to whom the authorising officer spoke, (normally the applicant), but should later be endorsed by the authorising officer (and Magistrate).

4.20 The authorisation should record:

- the reasons why the authorising officer or the officer entitled to act in urgent cases considered the case so urgent that an oral instead of a written authorisation was given and/or
- The reasons why it was not reasonably practicable for the application to be considered by the authorising officer.

4.21 Urgent authorisations unless renewed cease to have effect after seventy two hours beginning with the time when the authorisation was granted.

Necessity

4.22 Surveillance operations shall only be undertaken where there is no reasonable and effective alternative way of achieving the desired objective(s).

Effectiveness

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

Proportionality

4.24 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. Proportionate must also include whether it is a potential criminal offence that could attract a custodial sentence of six months or more, or involves the sales of tobacco or alcohol to minors.

Authorisation

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

Time Periods -Authorisations

4.26 Oral applications expire after 72 hours. If required they can be renewed for a further period of 3 months if renewed in writing.

4.27 Written authorisations expire 3 months beginning on the day from which they took effect.

Time Periods - Renewals

4.28 If at any time before an authorisation would expire, (including oral authorisations), 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.

4.29 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.

4.30 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 fare obtained by the surveillance
- The results of regular reviews of the investigation or operation

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. The 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.

Cancellation

4.32 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.

4.33 The cancellation should include how the surveillance assisted the investigation and details regarding direction of the product.

Monitoring

4.34 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

4.35 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 Code of Practice.

4.36 The Chief Internal Auditor will create and maintain 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.

4.37 The Chief Internal Auditor shall also retain 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 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.

4.38 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.

4.39 Generally the Chief Internal Auditor will retain all original forms for at least three years from the date of cancellation. In all cases records will not be destroyed without the authority of the Responsible Senior 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

Authorisation for CHIS

5.4 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.

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

5.6 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.

5.7 Where a CHIS is used the following records must be kept (in accordance with SI 2000 No 2725) 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.

5.8 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.

Juvenile Sources/Vulnerable Individuals

5.9 Special safeguards apply to the use or conduct of a juvenile CHIS (i.e. under 18 year olds). On no occasion can a child under 16 years of age be authorised to give information against his or her parents or any person who has parental responsibility for them. The duration of any authorisation is one month from the time of grant or renewal (instead of twelve months).

5.10 A vulnerable individual is a person who is or may be in need of community care services by reason of mental or other disability, age or illness and who is or may be unable to take care of himself or herself, or unable to protect himself or herself against significant harm or exploitation.

5.11 A vulnerable individual will only be authorised to act as a source in the most exceptional of circumstances and a juvenile source or vulnerable individual source will only be authorised by the Chief Executive Officer (David Williams) or the person acting as the Head of Paid Service in his absence.

Please Note: Any use of a CHIS in any capacity requires the completion of a risk assessment and authority from your Section Managers or Head of Service. In the case of Juveniles or Vulnerable individuals this is particularly so and these applications may only be authorised by the Chief Executive.

Test Purchases and CHIS's

5.12 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.

5.13 However, developing a relationship with a person in the shop, to obtain information about the sellers suppliers of an illegal product e.g. illegally imported products will require authorisation as a CHIS. Similarly, using mobile, hidden recording devices or COW 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 a separate directed surveillance authorisation.

6. CCTV

6.1 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.

7. COMMUNICATIONS DATA

Definition

7.1 The Regulation of Investigatory Powers (Communications Data) Order 2003 extends to local authorities the powers set out within RIPA to access communications data. Communications data includes information relating to the use of a communications service but does not include the contents of the communications itself (see section 21(4) RIPA for the detailed definition of "communications data").

7.2 Local authorities are allowed to access communications data only for the purposes of the prevention or detection of crime or the prevention of disorder.

7.3 Portsmouth City Council is only entitled to access:

(i) **Subscriber ("Customer') data** being any information, which does not include any of the contents of a communication, about the use made by any person of a postal or telecommunications service. In respect of a telecommunications service

provider this is normally referred to as the "billing information").
This will include:

- Name of subscriber
- Address for billing, delivery or installation
- Contact telephone numbers
- Abstract personal data provided by the subscriber e.g. demographic information
- Subscriber account information e.g. billing arrangements including bank, credit/debit card details Other services provided to the customer

(ii) **Service data** being any other information held by the service provider relating to the persons to whom the service is provided. (This is normally referred to as "subscriber information").
This will include:

- The period during which the customer used the service Information about forwarding services provided by telecommunication service providers and re-direction services provided by postal service providers.
- Itemised billing information. Information on connection, disconnection and redirection Information on conference calls, call messaging, call waiting and call barring services
- Top-up details for pre-pay mobile phones including credit/debit cards used
- For postal items, records of registered, recorded or special delivery of postal items and the delivery or collection of parcels.

Accessing Communications Data

7.4 Access to communications data may be authorised in two ways; either (a) through an authorisation by a designated person which would allow the authority to collect or retrieve data itself, or (b) by a notice given to a postal or telecommunications operator requiring that operator to collect or retrieve the data and provide it to the local authority.

7.5 There is a Code of Conduct, which refers to a "Designated Person" granting authorisation or giving notices in relation to accessing Communication Data. Portsmouth City Council use the National Anti Fraud Network (NAFN) as the SPOC (Single Point of Contact) and applications are sent to them for authorisation but the investigating officer must still seek magisterial approval.

8 IMPACT RISK ASSESSMENT

8.1 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.

8.2 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**

8.3 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?

8.4 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?

8.5 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.

8.6 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

9. FURTHER GUIDANCE

9.1 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
Flowchart 4: Duration of authorisation and renewals
Surveillance an aid to investigation Guidance

9.2 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.

9.3 In an urgent case telephone authorisation may be granted but both parties must then complete the written application and authorisation. The forms contain guidance on the information that must be provided in order to comply with the law.

10. OVERSIGHT

Senior Responsible Officer

10.1 The Senior Responsible Officer (at Portsmouth City Council this is Michael Lawther the City Solicitor and Monitoring Officer) must review each authorised RIPA to ensure that they are being authorised in accordance with the Code and to identify any training requirements.

Members

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

10.3 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.

Office of Surveillance Commissioners

10.4 The Office of Surveillance Commissioners, (OSC), 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 OSC.

11 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
SWLH 9ZQ
Tel: 020 7273 4514