Southampton City Council
Corporate Surveillance Guidance
The Regulation of Investigatory Powers Act 2000
August 2022

SOUTHAMPTON
CITY COUNCIL

Southampton City Council
Corporate Surveillance Guidance
The Regulation of Investigatory Powers Act 2000
August 2022

Contents

Corporate Surveillance Guidance			
Version	17.0	**Approved by**	Director of Legal & Business Services
Date last amended	27th July 2020	**Approval date**	26th September 2022
Lead officer	Tracy Horspool, Senior Solicitor (Corporate)	**Review date**	26th September 2023
Contact	information@southampton.gov.uk	**Effective date**	26th September 2022

1. Introduction

1.1 Summary

The Regulation of Investigatory Powers Act 2000 ('RIPA') brought into force the regulation of covert investigation by a number of bodies, including local authorities. RIPA regulates a number of investigative procedures, the most recent of which is the access to communications data.

This document is intended to provide officers with guidance on the use of covert surveillance, Covert Human Intelligence Sources ('Sources') and the obtaining and disclosure of communications data under RIPA. Officers must take into account the Codes of Practice issued under RIPA (RIPA and the Codes of Practice may be found at www.security.homeoffice.gov.uk).

1.2 Background

The Human Rights Act 1998 requires the Council, and organisations working on its behalf, pursuant to Article 8 of the European Convention, to respect the private and family life of a citizen, his home and his correspondence.

The European Convention did not, however, make this an absolute right, but a qualified right. Accordingly, in certain circumstances, the Council may interfere in the citizen's right mentioned above, if such interference is:

(a) in accordance with the law
(b) necessary (as defined in this document); and
(c) proportionate (as defined in this document).

RIPA provides a statutory mechanism for authorising certain types of surveillance. It seeks to ensure that any interference with an individual's right under Article 8 of the European Convention is necessary and proportionate. In doing so, RIPA seeks to ensure both the public interest and the human rights of individuals are suitably balanced.

If the correct procedures are not followed, evidence may be disallowed by the courts, a complaint of maladministration could be made to the Ombudsman, and/or the Council could be ordered to pay compensation. It is essential, therefore, that all

involved with RIPA comply with this document and any further guidance that may be issued, from time to time, by the Director of Legal & Business Services.

Each officer of the Council with responsibilities for the conduct of investigations, shall, before carrying out any investigation involving RIPA, undertake appropriate training to ensure that investigations and operations that he/she carries out will be conducted lawfully.

The Director of Legal & Business Services, is appointed as the senior responsible officer to ensure the integrity of the process within the Council and its compliance with RIPA; to have oversight of reporting of errors to the relevant oversight commissioner; responsibility for engagement with the Investigatory Powers Commissioner's Office when they conduct their inspections and where necessary, oversight of the implementation of any post-inspection action plan. The senior responsible officer will also ensure that Members regularly review the Council's use of RIPA.

1.3 Review

RIPA and this document are important for the effective and efficient operation of the Council's actions with regard to surveillance. This document will, therefore be kept under yearly review by the Director of Legal & Business Services.

Authorising Officers must bring any suggestions for continuous improvement of this document to the attention of the Director of Legal & Business Services, at the earliest possible opportunity.

1.4 Scope

RIPA covers the authorisation of directed surveillance, the authorisation of sources and the authorisation of the obtaining of communications data. Communications data includes information relating to the use of a postal service or telecommunications system but does not include the contents of the communication itself, contents of e-mails or interaction with websites. An authorisation under RIPA will provide lawful authority for the investigating officer to carry out surveillance.

In terms of monitoring e-mails and internet usage, it is important to recognise the interplay and overlaps with the Council's e-mail and internet policies and guidance, the Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000 and the Data Protection Act 2018. RIPA forms should be used where relevant and they will only be relevant where the criteria listed on the forms are fully met.

2. General

2.1 Definition of Surveillance

'Surveillance' includes:

a) monitoring, observing or listening to persons, their movements, their conversations or their other activities or communication;
b) recording anything monitored, observed or listened to in the course of surveillance; and
c) surveillance by or with the assistance of a surveillance device.

Surveillance includes the interception of postal and telephone communications where the sender or recipient consents to the reading of or listening to or recording of the communication. This is a form of directed surveillance.

2.2 Confidential Material

Particular care should be taken in cases where the subject of the investigation or operation might reasonably expect a high degree of privacy, or where confidential information is involved. Confidential information consists of matters subject to legal privilege, confidential personal information, confidential journalistic material and communications between an MP and a constituent.

Applications in which the surveillance is likely to result in the acquisition of confidential material will only be considered in exceptional and compelling circumstances with full regard to the proportionality issues this raises.

The Authorising Officer shall give the fullest consideration to any cases where the subject of the surveillance might reasonably expect a high degree of privacy, for instance in his or her home.

Where a likely consequence of surveillance would result in the acquisition of confidential material, the investigating officer must seek authority from the Chief Executive, or, in his absence, the Director of Legal & Business Services.

3. Directed and intrusive surveillance

3.1 Directed Surveillance

Directed surveillance is surveillance which is covert, but not intrusive, and undertaken:

a) for the purposes of a specific investigation or specific operation;

b) in such a manner as is likely to result in the obtaining of private information about a person (whether or not one specifically identified for the purposes of the investigation or operation); and

c) otherwise than by way of an immediate response to events or circumstances the nature of which is such that it would not be reasonably practicable for an authorisation under RIPA to be sought for the carrying out of the surveillance.

3.2 Intrusive Surveillance

That surveillance becomes intrusive if the covert surveillance:

a) is carried out by means of a surveillance device in relation to anything taking place on any residential premises or in any private vehicle; or

b) is carried out without that device being present on the premises or in the vehicle, is not intrusive unless the device is such that it consistently provides information of the same quality and detail as might be expected to be obtained from a device actually present on the premises or in the vehicle, or

c) is carried out in places ordinarily used for legal consultation, at a time when they are being used for such consultations

Therefore, directed surveillance turns into intrusive surveillance if it is carried out involving anything that occurs on residential premises or any private vehicle and involves the presence of someone on the premises or in the vehicle or is carried out by means of a surveillance device **OR** when directed surveillance is carried out in places ordinarily used for legal consultation, at a time when they are being used for such consultations.

For intrusive surveillance relating to residential premises or private vehicles, if any device used is not on the premises or in the vehicle, it is only intrusive surveillance if it consistently produces information of the same quality as if it were.

Where covert surveillance is carried out by a device designed or adapted principally for the purpose of providing information about the location of a vehicle, the activity is directed surveillance.

Commercial premises and vehicles are therefore excluded from intrusive surveillance. Currently, local authorities are **not** authorised to carry out intrusive surveillance.

4. Identifying directed surveillance

Ask yourself the following questions:

4.1 Is the surveillance covert?

Covert surveillance is any surveillance that is carried out in a manner calculated to ensure that the persons subject to the surveillance are unaware that it is or may be taking place.

If your activities are not hidden from the subjects of your investigation, you are not within the RIPA framework at all. In many cases, Officers will be behaving in the same way as a normal member of the public (e.g. in the case of most test purchases), and/or will be going about Council business openly (e.g. a market inspector walking through markets).

Similarly, surveillance will be overt if the subject has been told it will happen (e.g. where a noisemaker is warned (preferably in writing) that noise will be recorded if the noise continues, or where an entertainment licence is issued subject to conditions, and the licensee is told that officers may visit without notice or identifying themselves to the owner/proprietor to check that conditions are being met.

It should be noted that if the same outcome can be achieved by overt means then those means need to be fully explored in the first instance. Covert surveillance must only be undertaken when there is no less invasive way of achieving the outcome.

4.2 Is the surveillance for the purposes of a specific investigation or a specific operation?

Although, the provisions of the Act do not normally cover the use of overt CCTV surveillance systems, since members of the public are aware that such systems are in use, there may be occasions when public authorities use overt CCTV systems for the purposes of a specific investigation or operation. For example, if the CCTV cameras are targeting a particular known offender. In such cases, authorisation for directed surveillance may be necessary.

4.3 Is the surveillance in such a manner that is likely to result in the obtaining of private information about a person?

Private information includes any information relating to a person's private or family life. The concept of private information should be broadly interpreted to include an individual's private or personal relationship with others. It includes an individual's business and family relationships. Family life itself should be treated as extending beyond the formal relationships created by marriage.

4.4 Is the surveillance otherwise than by way of an immediate response to events or circumstances where it is not reasonably practicable to get authorisation?

Directed surveillance does not include covert surveillance carried out by way of an immediate response to events or circumstances which, by their very nature, could not have been foreseen. For example, a police officer would not require an authorisation to conceal himself and observe a suspicious person that he came across in the course of a patrol.

However, if as a result of that immediate response, you undertake a specific investigation you will need authorisation.

5. Covert human intelligence sources

5.1 Definition

A person is a source if:

a) he establishes or maintains 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) he covertly uses such a relationship to obtain information or to provide access to any information to another person; or

c) he covertly discloses information obtained by the use of such a relationship or as a consequence of the existence of such a relationship.

A source may include those referred to as agents, informants and officers working undercover.

A purpose is covert, in relation to the establishment or maintenance of a personal or other relationship, if and only if, the relationship is conducted in a manner that is calculated to ensure that one of the parties to the relationship is unaware of the purpose.

A relationship is used covertly, and information obtained is disclosed covertly, if and only if it is used or 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.

The use of a source involves inducing, asking or assisting a person to engage in the conduct of a source, or to obtain information by means of the conduct of such a source.

This covers the use of professional witnesses to obtain information and evidence. For example, it will include professional witnesses retained by Housing to pose as tenants to obtain information and evidence against alleged nuisance perpetrators.

Carrying out test purchases will not 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).

By contrast, developing a relationship with a person in the shop, to obtain information about the seller's suppliers of an illegal product will require authorisation as a CHIS. Similarly, using mobile hidden recording devices or CCTV cameras to record what is going on in the shop, or an adult is observing a juvenile test purchase, this will require authorisation as directed surveillance. In all cases, a prior risk assessment is essential in relation to any young person used for a test purchase.

The Code of Practice states that the provisions of RIPA are not intended to apply in circumstances where members of the public volunteer information to the police or other authorities, as part of their normal civic duties, or to contact numbers set up to receive information (such as Crimestoppers, Customs Confidential, the Anti Terrorist Hotline, or the Security Service Public Telephone Number). Members of the public acting in this way would not generally be regarded as sources.

It should be noted, however, that if the information provided is recorded as potentially useful or actionable, there is potential duty of care to the individual and the onus is on the public authority to manage human sources properly. Authorising Officers should be alive to the possibility of 'status drift'. Authorising Officers, when deciding whether to grant an authorisation, should take account of the difference between a volunteer of information already known to the individual and the relevance of the exploitation of a relationship for a covert purpose.

An authorisation under RIPA will provide lawful authority for the use of a source.

5.2 Security and Welfare

Only the Chief Executive or, in his absence, the Director of Legal & Business Services, is able to authorise the use of vulnerable individuals and juvenile sources. The Authorising Officer shall have regard to the special safeguards and provisions that apply to vulnerable individuals and juvenile sources, more particularly set out in the Covert Human Intelligence Source Code of Practice at www.security.homeoffice.gov.uk.

The Authorising Officer shall ensure that arrangements are in place for the proper oversight and management of sources, including appointing individual officers for each source. The person responsible for the day-to-day contact between the public authority and the source will usually be of a rank or position below that of the Authorising Officer.

Officers using a source shall consider the safety and welfare of that source (even after cancellation of the authorisation), and the foreseeable consequences to others of the tasks they are asked to carry out. The Authorising Officer shall carry out a risk assessment before authorising the source.

6. Covert surveillance of social networking sites (SNS)

6.1 Even though data may be deemed published and no longer under the control of the author, it is unwise to regard it as 'open source' or publicly available. The author has a reasonable expectation of privacy if access controls are applied. In some cases, data may be deemed private communication still in transmission.

6.2 Providing there is no warrant authorising interception in accordance with section 48(4) of the Act, if it is necessary and proportionate for a public authority to breach covertly access controls, the minimum requirement is an authorisation for directed surveillance. An authorisation for the use and conduct of a CHIS is necessary if a relationship is established or maintained by a member of a public authority or by a person acting on its behalf, i.e. the activity is more than mere reading of the site's content

6.3 Officers must not:

- Set up a false identity for a covert purpose without authorisation
- Adopt the identity of a person known, or likely to be known, to the subject of interest or users of the site without authorisation and without the consent of the person of the person whose identity is used, and without considering the protection of that person. The consent must be explicit.
- Use their personal social network login details to view individuals under investigation

6.4 In deciding whether online surveillance should be regarded as covert, consideration should be given to the likelihood of the subject(s) knowing that the surveillance is or may be taking place. Use of the internet itself may be considered as adopting a surveillance technique calculated to ensure that the subject is unaware of it, even if no further steps are taken to conceal the activity. Conversely, if reasonable steps have been taken to inform the public or particular individuals that the surveillance is or may be taking place, this can be regarded as overt and a directed surveillance authorisation will not normally be available.

6.5 As set out in paragraph 6.6 below, depending on the nature of the online platform, there may be a reduced expectation of privacy where information relating to a person or group of people is made openly available within the public domain, however in some circumstances privacy implications still apply. This is because the intention when making such information available was not for it to be used for a covert purpose such as investigative activity. This is regardless of whether a user of a website or social media platform has sought to protect such information by restricting its access by activating privacy settings.

6.6 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.

6.7 Whether the Council interferes with a person's private life includes a consideration of the nature of the Council'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 the Council is systematically collecting and recording information about a particular person or group, a directed surveillance authorisation should be considered. These considerations apply regardless of when the information was shared online.

Example 1: A simple internet search on a name, address or telephone number to find out whether a subject of interest has an online presence is unlikely to need an authorisation. However, if having found an individual's social media profile or identity it is decided to monitor it or extract information from it for retention in a record because it is relevant to an investigation or operation, authorisation should then be considered.

Example 2: Initial examination of an individual's online profile to establish whether they are of relevance to an investigation is unlikely to need an authorisation. Visiting a website would not normally amount to surveillance, but if during that visit it is intended to extract and record information to establish a profile including information such as identity, pattern of life, habits, intentions or associations, it may be advisable to have in place an authorisation even for that single visit. As set out in the following paragraph, the purpose of the visit may be relevant as to whether an authorisation should be sought.

Example 3: General monitoring of the internet in circumstances where it is not part of a specific, ongoing investigation or operation does not require RIPA authorisation. This includes any monitoring that is intended to identify themes, trends, possible indicators of criminality or other factors that may influence operational strategies or deployments. It may also include the discovery of previously unknown subjects of interest, but once it is decided to monitor those individuals as part of an ongoing operation or investigation, authorisation should be considered.

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

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

10

6.9 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

Example: Researchers within a public authority using automated monitoring tools to search for common terminology used online for illegal purposes will not normally require a directed surveillance authorisation. Similarly, general analysis of data by public authorities either directly or through a third party for predictive purposes (e.g. identifying crime hotspots or analysing trends) is not usually directed surveillance. In such cases, the focus on individuals or groups is likely to be sufficiently cursory that it would not meet the definition of surveillance. But officers should be aware of the possibility that the broad thematic research may evolve, and that authorisation may be appropriate at the point where it begins to focus on specific individuals or groups. If specific names or other identifiers of an individual or group are applied to the search or analysis, an authorisation should be considered.

6.10 Each viewing of a company or an individual's Social Media profile for the purpose of investigation or evidence gathering must be notified to the senior responsible officer and will be recorded on the log held by the Corporate Legal Team. All Authorising Officers have access to view the log on Sharepoint.

7. Communications data

7.1 Definition

This covers any conduct in relation to a postal service or telecommunications system for obtaining communications data and the disclosure to any person of such data. For these purposes, communications data includes information relating to the use of a postal service or telecommunications system but does not include the contents of the communication itself, content of emails or interaction with websites.

Communications data includes subscribers details, names and addresses and telephone numbers of those contacted, billing addresses, account information, web addresses visited etc.

The Investigatory Powers Act 2016 (IPA) created new Communications Data terminology. Communications Data now comprises 'Entity Data' and 'Events Data'.

Entity Data broadly replaces 'Subscriber Data' under RIPA, s21(4)(c), e,g name of subscriber, address for billing, contact telephone number, subscriber account information etc.

Events Data identifies or describes events which consist of one or more entities engaging in an activity at a specific time or times. It includes call histories and activity, including itemized records of telephone calls, internet connections, dates and times/duration of calls etc. Event data refers to both 'Traffic Data' (S21(4)(a)) and 'Service Use Information' (S21(4)(b)) under RIPA. Where the purpose of the acquisition is to prevent or detect crime and the data required is Events data, the offence or conduct of the offence being investigated must meet at least one of the definitions of serious crime.

7.2 Serious Crime threshold

From 1st November 2018, an amendment to RIPA came into force adding a serious crime threshold to the acquisition of service or traffic data. This means that where an application is for the crime statutory purpose (S60A(7)(b)) to acquire event data, the crime must be a serious crime.

7.3 Definition of Serious Crime

- 12 months (or more) imprisonment
  - an offence that is capable of attracting a prison sentence of 12 months or more
- Corporate Body
  - an offence by a person who is not an individual
- S81 Offence
  - an offence falling within the definition of serious crime in S81(3)(b) of the IPA where the conduct involves the use of violence, results in substantial financial gain or is by a large number of persons in pursuit of a common

purpose

- Communication Offence
  - an offence which involves, as an integral part of it, the sending of a communication
- Breach of Privacy
  - an offence which involves, as an integral part of it, a breach of a person's privacy

8. Authorisation procedure

8.1 General

Authorisation is required for the use of directed surveillance, for the conduct and use of sources and for the conduct in relation to a postal service or telecommunication system and the disclosure to any person of such data. Authorisation for directed surveillance can only be granted if the purpose of the surveillance is the prevention or detection of crime(s) punishable by 6 months imprisonment or more, or relates to the sale or alcohol or tobacco to underage persons.

All applications for authorisation of directed surveillance or for the conduct and use of any source must be referred to the RIPA Co-Ordinator (Senior Solicitor-Corporate legal Team) before submission by the Co-Ordinator to an Authorising Officer for consideration.

If the authorisation is provisionally approved by the Authorising Officer, each provisional authorisation then needs to receive judicial approval before being acted upon. Once approved, the original authorisation and accompanying paperwork must be forwarded to the RIPA Co-Ordinator (Senior Solicitor – Corporate Legal Team) to allocate the application a Unique Reference Number (URN) and for key details to be entered onto the central register. For further detail, see paragraph 12.1.

Any officer wishing to engage in conduct in relation to a postal service and telecommunication system for obtaining communications data and the disclosure to any person of such data must also seek authorisation, the procedure of which differs slightly and is outlined in paragraph 8.5.

8.2 Who can give Provisional Authorisations?

By law, the 'Authorising Officer' for local authority purposes is any assistant Chief Officer, assistant Head of Service, service manager or equivalent. An Authorising Officer may grant a provisional authorisation, but this authorisation will not take effect until it receives judicial approval (See paragraph 7.4). More senior officers within a Council may also give provisional authorisations in the circumstances to those whom they are senior. Please note that certain provisional authorisations, namely those relating to confidential information, vulnerable individuals and juvenile sources, can

only be granted by the Chief Executive, or, in his genuine absence, the Director of Legal & Business Operations.

The Council's authorised posts are listed in Appendix 1. This appendix will be kept up to date by the Director of Legal & Business Operations and added to as needs require. If a Chief Officer wishes to add, delete or substitute a post, a request must be referred to the Director of Legal & Business Operations, for consideration as necessary. The Service Director, Legal & Governance, has the delegated authority to add, delete or substitute posts.

It will be the responsibility of Authorising Officers who have been duly certified to ensure their relevant members of staff are also suitably trained as 'applicants' so as to avoid common mistakes appearing on forms for RIPA authorisations.

Training will be given, or approved by the Director of Legal & Business Operations, before Authorising Officers are certified to sign any RIPA forms. A certificate of training will be provided to the individual and a central register of all those individuals who have undergone training or a one-to-one meeting with the Director of Legal & Business Operations, on such matters, will be kept by the Director of Legal & Business Operations.

Authorising officers should not normally be responsible for authorising operations in which they are directly involved, although it is recognised that this may sometimes be unavoidable. Where an Authorising Officer authorises such an investigation or operation the central register will highlight this and the Commissioner or inspector will be notified of this during his or her next inspection

Authorising Officers will also ensure that staff who report to them follow this guidance document and do not undertake or carry out any form of surveillance without first obtaining the relevant authorisations in compliance with this document.

Authorising Officers must also ensure that, when sending copies of authorisations and associated documentation to the Service Director, Legal & Governance, the same are sent in sealed envelopes and marked 'Strictly Private and Confidential'.

Any equipment to be used in any approved surveillance must be properly controlled, recorded and maintained for audit purposes.

8.3 Grounds for Authorisation – the 'necessary & proportionate' test

An Authorising Officer has a number of obligations within the provisions of the Act, which must be met before carrying out any form of surveillance.

An Authorising Officer shall not grant a provisional authorisation for the carrying out of directed surveillance, or for the use of a source or for the obtaining or disclosing of communications data unless he believes:

a) that a provisional authorisation is necessary and

b) the provisionally authorised investigation is proportionate to what is sought to be achieved by carrying it out

For local authority investigations, provisional authorisation is deemed "**necessary**" in the circumstances of the particular case if it is for the purpose of preventing and detecting crime or of preventing disorder.

Conduct is not deemed "**proportionate**" if the pursuance of the legitimate aim listed above will not justify the interference if the means used to achieve the aim are excessive in the circumstances. Any conduct must meet the objective in question and must not be arbitrary or unfair nor must the impact on any individuals or group be too severe.

The conduct must also be the least invasive method of achieving the end and the risk of intrusion into the privacy of persons other than those who are directly the subjects of the investigation must be assessed and taken into account (see Collateral Intrusion below).

Consideration must be given to the seriousness of the offence under consideration. Authorisation for directed surveillance can only be granted if the purpose of the surveillance is the prevention or detection of crime(s) punishable by 6 months imprisonment or more, or relates to the sale or alcohol or tobacco to underage persons. Covert surveillance relating to dog fouling and schools admissions/suspected false addresses will not be deemed a proportionate activity.

Careful consideration needs to be made by authorising officers of all of these points. Such consideration needs to be demonstrated on the authorisation form in the relevant parts. Authorising Officers must exercise their minds every time they are asked to sign a form. They must never sign or rubber stamp the form without thinking about their personal and the Council's responsibilities.

Any boxes not needed on the form/s must be clearly marked as being 'not applicable' or a line put through the same. Great care must also be taken to ensure accurate information is used and inserted in the correct boxes. Reasons for any refusal of an application must also be kept on the form and retained for future audits.

Authorising Officers should not be responsible for authorising investigations or operations in which they are directly involved.

Collateral Intrusion

Before provisionally authorising investigative procedures, the Authorising Officer shall also take into account the risk of intrusion into the privacy of persons other than those who are directly the subjects of the investigation or operation (collateral intrusion). The investigating officer shall take measures, wherever practicable, to avoid or minimise unnecessary intrusion into the lives of those not directly connected with the investigation or operation.

An application for a provisional authorisation shall include an assessment of the risk of any collateral intrusion. The Authorising Officer shall take this into account, when considering the proportionality of the surveillance.

Where an operation unexpectedly interferes with the privacy of individuals who were not the subject of surveillance or covered by the authorisation in some other way, the investigating officer should inform the Authorising Officer.

8.4 Judicial Approval of Provisional Authorisations and Renewals

The Council is only able to grant a provisional authorisation or renewal to conduct covert surveillance. All provisional authorisations and renewals must be approved by the Magistrates Court before surveillance commences.

The Council must apply to the local Magistrates Court for an Order approving the grant or renewal of an authorisation. A template application form and draft Order are included at Appendix 5 to this policy. In order to obtain judicial approval, the first page of the template form must be completed and submitted along with a copy of the provisional authorisation and any other relevant supporting documents.

The Council does not need to give notice of the application to the person(s) subject to the application or their legal representatives. If the Magistrates Court refuse to approve the application, they may also make an order quashing the provisional authorisation.

The Magistrates will consider the provisionally authorised application or renewal, and will need to satisfy themselves that:

a) At the time of provisional authorisation, there were reasonable grounds for believing that the tests of necessity and proportionality were satisfied in relation to the authorisation, and that those grounds still exist;

b) That the person who granted provisional authorisation was an appropriately designated person;

c) The provisional grant or renewal of any authorisation or notice was not in breach of any restrictions imposed under RIPA; and

d) Any other conditions provided for by an order made by the Secretary of State were satisfied.

A further requirement in relation to renewal of covert human intelligence sources, is that judicial approval will only be granted if the Magistrates are satisfied that a review has been carried out, which considers:

- the use made of the source in the period since authorisation was granted (or the last renewal); and
- the tasks given to the source during that period, and the information obtained from the conduct or use of the source.

and for the purposes of making an Order, the Magistrates have considered the results of that review.

The Council's Trading Standards Team will generally make applications for judicial approval to the Magistrates Court on behalf of the Council. Any particularly complex authorisations or authorisations arising from other areas of the Council that require legal input or representation may be dealt with by the Council's Legal Team if necessary in the circumstances.

8.5 Special Procedure for Authorisation in respect of Communications Data

8.5.1 The introduction of the Office for Communications Data Authorisations (OCDA) means the acquisition of Communications Data by local authority officers is no longer subject to judicial approval by a Magistrate. OCDA assesses Communications Data applications from public authorities and makes decisions about those applications that strike a fine balance between the protection of privacy and the risk to public safety. OCDA acts as a hub of authorisation expertise, independently assessing applications, holding authorities accountable to robust safeguarding standards and challenging where required.

8.5.2 Applications for the obtaining and disclosure of communications data may only be made by officers of the City Council.

8.5.3 Applications for communications data must be channelled through single points of contact ("SPoCs"). The SPoC is able to advise authorising officers as to whether an authorisation or notice is appropriate.

The City Council use the services of the National Anti-Fraud Network (NAFN) for all Communications Data enquiries and as such NAFN performs the role of a SPoC through their qualified SPoC officers. All applicants must be registered with NAFN via the NAFN website at www.nafn.gov.uk . Any initial internal queries can be directed to Tracy Horspool, Senior Solicitor (Corporate) at tracy.horspool@southampton.gov.uk .

8.5.4 The SPoC is required to:

- provide quality assurance checks to ensure that applications consistently comply with IPA standards and to a sufficient level to meet OCDA and IPCO scrutiny
- monitor those applications which are returned for rework or rejected by OCDA and determine the reasons why
- provide organisational and/or individual training as and where necessary sharing best practice, advice and support
- be the point of contact between public authorities and OCDA

8.5.5 S60A of IPA provides for independent authorisation of communications data requests by the Investigatory Powers Commissioner (IPC). OCDA performs this function on behalf of the IPC. An authorising officer in OCDA can authorise any lawful request, for any of the specified purposes from any listed authority. For the City Council, the sole purpose is the 'applicable crime purpose'.

8.5.6 The IPA provides a new requirement for a local authority making an application to ensure someone of at least the rank of Senior Responsible Officer is aware.

8.5.7 OCDA will only retain, for a limited period of time, the Communications Data applications which are sent to them and the decision document they issue back to public authorities. Public Authorities are therefore required to keep records of both the Communications Data applications that they issue as well as the decisions received from OCDA. Communications data, and all copies, extracts and summaries of it must be handled and stored securely. The requirements of the Data Protection Act 2018 and the principles of the Criminal Procedure and Investigations Act 1996 must be strictly followed.

8.5.8 Where the purpose of a Communications Data application is to identify a journalistic source, these must first be authorized by an Authorising Individual (OCDA AO or DSO) but must also be approved by an IPCO Judicial Commissioner (JC). The Applicant and SPOC should pay special consideration to these applications and inform their Senior Responsible Officer. The IPA does not alter the existing processes for Communications Data applications that may feature sensitive professions including medical doctors, lawyers, journalists, parliamentarians or ministers of religion. If the Communications Data could contain information relating to any of these professions, this must be noted in the application.

8.6 Urgency

Urgent authorisations are no longer available in relation to directed surveillance or covert human intelligence sources.

8.7 Standard Forms

All authorisations must be in writing.

Standard forms for seeking provisional directed surveillance and source authorisations are provided at Appendices 3 & 4. The standard form for obtaining judicial approval is provided at Appendix 5. All authorisations shall be sought using the standard forms as amended from time to time.

9. Activities by other public authorities

9.1 The investigating officer shall make enquiries of other public authorities e.g. the police whether they are carrying out similar activities if he considers that there is such a possibility in order to ensure that there is no conflict between the activities of this Council and those other public authorities.

10. Joint investigations

10.1 When some other agency has been instructed on behalf of the City Council to undertake any action under RIPA, this document and the forms in it must be used (as per normal procedure) and the agency advised or kept informed, as necessary, of the various requirements. They must be made aware explicitly what they are authorised to do.

When some other agency (e.g. police, Customs & Excise, Inland Revenue etc.):

(a) wish to use the City Council's resources (e.g. CCTV surveillance systems), that agency must use its own RIPA procedures and, before any officer agrees to allow the Council's resources to be used for the other agency's purposes, he must obtain a copy of that agency's RIPA form for the record and/or relevant extracts from the same which are sufficient for the purposes of protecting the Council and the use of its resources

(b) wish to use the Council's premises for their own RIPA action, the officer should, normally, co-operate with the same, unless there are security or other good operational or managerial reasons as to why the Council's premises should not be used for the agency's activities. In such cases, the Council's own RIPA forms should not be used as the Council is only assisting and not being involved in the RIPA activity of the external agency being involved in the RIPA activity of the external agency.

In terms of (a), if the police or other agency wish to use the Council's resources for general surveillance, as opposed to specific RIPA authorisations, an appropriate letter requesting the proposed use, remit, duration, details of who will be undertaking the general surveillance and the purpose of it must be obtained from the police or other agency before any Council resources are made available for the proposed use.

11. Duration, renewals and cancellation of authorisations

11.1 Duration

Authorisations must be reviewed in the time stated and cancelled once no longer needed.

Authorisations last for:

a) 12 months from the date of the judicial approval for the conduct or use of a source (4 months for juvenile CHIS authorisations)
b) three months from the date of judicial approval for directed surveillance
c) one month from the date of judicial approval for communications data,

or earlier if cancelled under Section 23(8) of the Act.

However, whether the surveillance is carried out/conducted or not in the relevant period, does not mean that the authorisation is spent. Authorisations do not expire, they have to be reviewed, or cancelled if no longer required.

11.2 Reviews

The Authorising Officer shall undertake regular reviews of authorisations to assess the need for the surveillance to continue. The results of a review should be recorded on the central record of authorisations.

Where the surveillance provides access to confidential information or involves collateral intrusion the officer should conduct frequent reviews.

Standard review forms for directed surveillance and CHIS are available on the RIPA intranet pages.

11.3 Renewals

Authorisations may be renewed more than once, if necessary, and the renewal should be kept/recorded as part of the central record of authorisations

Authorisations can be renewed in writing shortly before the maximum period has expired. An authorisation cannot be renewed after it has expired.

The Authorising Officer must consider the matter afresh, including taking into account the benefits of the surveillance to date and any collateral intrusion that has occurred.

The renewal will begin on the day when the authorisation would have expired, provided the necessary judicial approval has been obtained.

A further requirement in relation to renewal of covert human intelligence sources, is that judicial approval will only be granted if the Magistrates are satisfied that a review has been carried out, which considers:

- the use made of the source in the period since authorisation was granted (or the last renewal); and
- the tasks given to the source during that period, and the information obtained from the conduct or use of the source.

and for the purposes of making an Order, the Magistrates have considered the results of that review. The Authorising Officer who granted or last renewed the authorisation must cancel it if he is satisfied that the investigative procedure no longer meets the criteria upon which it was authorised.

Standard renewal forms for the authorisation of directed surveillance and CHIS are available on the RIPA intranet pages.

11.4 Cancellations

An Authorising Officer shall cancel a notice or authorisation as soon as it is no longer necessary, or the conduct is no longer proportionate to what is sought to be achieved. The duty to cancel a notice falls on the authorising officer who issued it.

In the case of a notice issued in respect of communications data, the relevant postal or telecommunications operator will be informed of the cancellation.

Standard cancellation forms for directed surveillance and CHIS are available on the RIPA intranet pages.

12. Records

The City Council must keep a detailed record of all authorisations, reviews, renewals, cancellations and rejections in departments and a central register of all such forms will be maintained by the Director of Legal & Business Services.

In relation to communications data, the designated SpoC will retain the forms and the Director of Legal & Business Services, will have access to such forms as and when required.

12.1 Central record of all Authorisations

The Director of Legal and Business Services, shall hold and monitor a centrally retrievable record of all provisional and judicially approved authorisations. The Authorising Officer must notify and forward a copy of any provisional notice or authorisation granted, renewed or cancelled and any judicial approval received or refused within 1 week of the event to the Director of Legal and Business Services to ensure that the records are regularly updated.

The record will be made available to the relevant Commissioner or an Inspector from the Investigatory Powers Commissioner's Office. These records will be retained for a period of 5 years from the ending of the authorisation. A record will be kept of the dates on which the authorisation notice is started and cancelled.

The Director of Legal & Business Services will monitor the submission of provisional and judicially approved authorisations and notices and give appropriate guidance, from time to time, or amend any provisional or draft document as necessary. The records submitted to the Director of Legal & Business Services, shall contain the following information:

a) the type of authorisation or notice
b) the date the provisional authorisation or notice was given;
c) name and rank/grade of the authorising officer;
d) the date judicial approval was received or refused;
e) the unique reference number (URN) of the investigation or operation;
f) the title of the investigation or operation, including a brief description and names of subjects, if known;
g) if the authorisation or notice is renewed, when it was renewed and who authorised the renewal, including the name and rank/grade of the authorising officer and the date of judicial approval;
h) whether the investigation or operation is likely to result in obtaining confidential information;
i) review dates
j) the date the authorisation or notice was cancelled
k) details of secure storage of surveillance data
l) stipulated period during which any surveillance data obtained must be reviewed, retained or destroyed

12.2 Records maintained in the Department

The Authorising Officer shall maintain the following documentation, which need not form part of the centrally retrievable record:

a) a copy of the application and provisional authorisation or notice together with a copy of any order of judicial approval or refusal, as well as any

supplementary documentation and notification of the approval given by the Authorising Officer;

b) a record of the period over which the surveillance has taken place;

c) the frequency of reviews prescribed by the Authorising Officer;

d) a record of the result of each review of the authorisation or notice;
e) a copy of any renewal of an authorisation or notice, together with judicial approval or refusal and the supporting documentation submitted when the renewal was requested;
f) the date and time when any instruction was given by the Authorising Officer;
g) the unique reference number for the authorisation (URN);
h) the stipulated period during which any surveillance data obtained must be reviewed, retained or destroyed

Each form must have a URN. The Authorising Officers will issue the relevant URN to applicants. The cross-referencing of each URN takes place within the form for audit purposes. Rejected forms will also have URN's.

12.3 Other Record of Covert Human Intelligence Sources

Proper records must be kept of the authorisation and use of a source. An Authorising Officer must not grant a provisional authorisation for the use or conduct of a source unless he believes that there are arrangements in place for ensuring that there is at all times a person with the responsibility for maintaining a record of the use made of the source. The records must be kept confidential. Further advice should be sought from the Director of Legal and Business Services on this point if authority is proposed to be granted for the use of a CHIS.

The records shall contain the following information:

(a) the identity of the source;
(b) the identity, where known, used by the source;
(c) any relevant investigating authority other than the Council;
(d) the means by which the source is referred to within each relevant investigating authority;
(e) any other significant information connected with the security and welfare of the source;
(f) any confirmation made by a person granting or renewing an authorisation for the conduct or use of a source that the information in paragraph (d) 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;
(g) the date when, and the circumstances in which, the source was recruited;
(h) the identities of the persons who, in relation to the source;
    i. hold day-to-day responsibility for dealing with the source and for the source's security and welfare
    ii. have a general oversight of the use made of the source (not to be the person identified in (h)(i))
    iii. have responsibility for maintaining a record of the use made of the source
(i) the periods during which those persons have discharged those responsibilities;
(j) the tasks given to the source and the demands made of him in relation to his

activities as a source;

(k) all contacts or communications between the source and a person acting on behalf of any relevant investigating authority;

(l) the information obtained by the conduct or use of the source;

(m) any dissemination of information obtained in that way; and

(n) in the case of a source who is not an undercover operative, every payment, benefit or reward and every offer of a payment, benefit or reward that is made or provided by or on behalf of any relevant investigating authority in respect of the source's activities for the benefit of that or any other relevant investigating authority.

13. Retention and destruction

13.1 Material obtained from properly authorised surveillance or a source may be used in other investigations. Arrangements shall be in place for the handling, storage, review and destruction of material obtained through the use of covert surveillance, a source or the obtaining or disclosure of communications data. Authorising Officers must ensure compliance with the appropriate data protection requirements, any legal constraints on destruction and the council's corporate policies relating to the handling and storage, review and destruction of material. The authorisation must stipulate the period during which the surveillance data may be retained, reviewed and destroyed. This will also be recorded on the central record of authorisations and in the records maintained in the department (see paragraphs 12.1 and 12.2).

13.2 Where the product of surveillance could be relevant to pending or future proceedings, it should be retained in accordance with established disclosure requirements for an appropriate period and subject to review. Reviews must be conducted at regular intervals to ensure that the justification for retention is still valid. Records shall generally be maintained for a period of 5 years from the cancellation of the authorisation, following which they shall be securely destroyed in accordance with the council's Records Review and Retention Schedule.

13.3 As detailed in paragraphs 12.2 and 12.3, Applicants and Authorising Officers must keep copies of completed RIPA forms, but care must be taken to ensure any copies are stored securely, reviewed and disposed of in accordance with the relevant legal framework and the council's Records Review and Retention Schedule. It is good practice for officers who will be carrying out surveillance to retain a copy of the authorisation as a reminder of exactly what has been authorised. Under the Criminal Procedure and Investigations Act 1996 and its Code of Parctice, case files are required to hold original documents for court action.

13.4 All data obtained under RIPA must be secured against unauthorised interference and clearly labelled and stored in such a way to enable compliance with data retention and disposal. This requirement will apply to information which is shared with other teams for the purpose of any investigation or to determine legal action to be undertaken.

13.5 All data obtained under RIPA must be stored in a secure manner using password protection or restricted access files. All RIPA records, whether in original form or copies shall be kept in secure locked storage when not in use. Storage must be in council premises to which access is restricted. Both physical and IT security, as appropriate, must be in place to secure the material.

13.6 A display of personal data or operational data on a computer screen should only take

place in a setting in which no unauthorised person is present.

13.7 Transmission of surveillance data must be limited to that strictly necessary for the purposes of the investigation. All recipients of data obtained under RIPA must be limited to such information as is strictly necessary for the purposes of the investigation and such information to be retained only as long as is necessary and in accordance with the council's Records Review and Retention Schedule. Review and disposal of data must be recorded on each occasion on the council's Records Review Log.

13.8 Officers within the same team who need to be aware of the investigation and have a demonstrable 'need to know', should be granted access to the data held on the relevant computer system (for example Uniform or Iken), rather than multiple copies of the data being emailed.

13.9 In the absence of a court order, disclosure to third parties, such as the police, can only be authorised by the council's senior responsible officer. Such disclosures must be recorded in writing and satisfy all legal tests. Disclosure must be the minimum necessary and only for an authorised purpose as set out below:

- is, or is likely to become, necessary for any of the statutory purposes set out in the RIPA Act in relation to covert surveillance or CHIS activity;
- is necessary for facilitating the carrying out of the functions of public authorities under RIPA;
- is necessary for facilitating the carrying out of any functions of the Commissioner or the Investigatory Powers Tribunal;
- is necessary for the purposes of legal proceedings; or
- is necessary for the performance of the functions of any person by or under any enactment.

14. Consequences of ignoring RIPA

14.1 RIPA states that if authorisation confers entitlement to engage in a certain conduct and the conduct is in accordance with the authorisation, then it shall be lawful for all purposes.

Where there is interference with the right to respect for private and family life guaranteed under Article 8 of the European Convention on Human Rights, and where there is no other source of lawful authority, the consequence of not obtaining an authorisation under RIPA may be that the action is unlawful by virtue of section 6 of the Human Rights Act 1998.

Officers shall seek an authorisation where the directed surveillance, the use of a source or the obtaining or disclosure of communications data is likely to interfere with a person's Article 8 rights to privacy by obtaining private information about that person, whether or not that person is the subject of the investigation or operation.

Obtaining an authorisation will ensure that the action is carried out in accordance with law and subject to stringent safeguards against abuse.

15. Scrutiny of investigatory bodies

15.1 The Investigatory Powers Commissioner's Office independently scrutinises the use of RIPA powers by the investigatory bodies that are subject to it.

The Commissioner will inspect Councils to ensure compliance with RIPA and can audit/review the Council's policies and procedures, and individual authorisations. Further detail can be found at www.ipco.org.uk

15.2 There is also a statutory complaints system welcomed by the Council. The Investigatory Powers Tribunal has been established under RIPA to deal with complaints from members of the public about the use or conduct by public authorities of these powers. The Tribunal is separate from IPCO.

The Council welcomes this external scrutiny. It expects its officers to co-operate fully with these statutory bodies and to bring forward any proposals for improvement that may follow on from an inspection report or a Tribunal hearing.

IF IN DOUBT ADVICE MUST BE SOUGHT FROM THE DIRECTOR OF LEGAL AND BUSINESS SERVICES OR THE CORPORATE LEGAL TEAM