Appendix 1

Policy and Procedures for undertaking Directed Covert Surveillance and the use of Covert Human Intelligence Sources

Produced by

- Internal Audit Services, April 2010
- Updated w 1st November 2012
- Updated May 2014
- Updated June 2016
- UPDATED OCTOBER 2016
- UPDATED SEPT 2018
- UPDATED SEPT 2019

CONTENTS

PART 1

POLICY FOR UNDERTAKING DIRECTED COVERT SURVEILLANCE AND USE OF COVERT HUMAN INTELLIGENCE SOURCES

PART 2

DETAILED PROCEDURES FOR UNDERTAKING DIRECTED COVERT SURVEILLANCE

PART 3

DETAILED PROCEDURES FOR USE OF COVERT HUMAN INTELLIGENCE SOURCES

PART 1

POLICY FOR UNDERTAKING DIRECTED COVERT SURVEILLANCE AND USE OF COVERT HUMAN INTELLIGENCE SOURCES

1. Introduction

1.1 The performance of certain investigatory functions of Local Authorities may require the surveillance of individuals or the use of informants Such actions may intrude on the privacy of individuals and can result in private information being obtained and as such, should not be undertaken without full and proper consideration. Legislation now governs how Local Authorities should administer and record surveillance and the use of informants and renders evidence obtained lawful for all purposes This Policy sets out the Council's rules and procedures

1 2 The purpose of this Policy is to ensure there is a consistent approach to the undertaking and authorisation of surveillance activity Therefore, this Policy is to be used by all Council service areas and officers undertaking investigation work and using the techniques of surveillance or the use of Covert Human Intelligence Sources (CHIS's)

1 3 In this Policy the following terms shall have the meanings stated·

"**Investigating Officer**" – shall mean any Council officer undertaking or wishing to undertake directed covert surveillance or to use a CHIS provided he / she has received appropriate training.

"**Authorising Officer**" – shall mean.

i) All Chief Officers who have received appropriate training
ii) Holders of the following three posts provided he/she has received appropriate training – Group Manager for Environmental Health, Group Manager Waste and Environmental Care and the Director for Public Protection

"**Senior Responsible Officer**" – shall mean the Executive Director (Legal & Democratic Services) John Williams
johnwilliams@southend.gov.uk

"Principal Legal Executive" – shall mean the officer with this job title currently Tessa O'Connell
tessaoconnell@southend.gov.uk

1 4 This Policy was updated in November 2012 to reflect the provisions of the Protection of Freedoms Act 2012 which from the 1st November 2012 requires that a Justice of the Peace ("JP") must approve all Local Authority RIPA applications and renewals

Two guidance documents explaining this authorisation process have been issued by the Home Office to Local Authorities and Magistrates and these are available on the following links

https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/118173/local-authority-england-wales.pdf

https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/118174/magistrates-courts-eng-wales.pdf

This Policy was updated in June 2016 to incorporate additional information on surveillance outside RIPA in Section 6 and regarding the internet and social media for research and investigations in Section 7

This Policy was updated in September 2018 to reflect the "Covert Surveillance and Property Interference Revised Code of Practice" issued by the Home Office ("the 2018 Code") and this can be accessed using the link below

https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/742041/201800802_CSPI_code.pdf

1 5 RIPA was overseen by the Office of Surveillance Commissioners (OSC) However, from 1 Sept 2017 oversight transferred to the Investigatory Powers Commissioner's Office (IPCO) IPCO is the independent inspection regime whose remit includes providing comprehensive oversight of the use of the powers to which the 2018 Code applies, and adherence to the practices and processes described in it IPCO also provides guidance to be followed which is separate from the 2018 Codes

1.6 This Policy is intended to be a best practice guide It is not intended to replace the 2018 Code and where necessary the Code should be consulted. However, following this Policy ensures compliance with the 2018 Codes

1 7 This Policy is not intended to be an exhaustive guide and specific legal advice should be sought if Council officers do not find questions answered after reading this document and the 2018 Code. Officers should always consult the Legal Team before seeking authorisation

2. Background

2 1 On 2nd October 2000 the Human Rights Act 1998 (HRA) came into force making it potentially unlawful for a Local Authority to breach any article of the European Convention on Human Rights (ECHR) Any such breach may now be dealt with by the UK courts directly, rather than through the European Court at Strasbourg

2 2 Article 8 of the ECHR states that everyone has the right to respect for his private and family life, his home and his correspondence. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of

- National security
- Public safety
- The economic well-being of the country
- The prevention of disorder or crime
- The protection of health or morals
- The protection of the rights and freedoms of others

2.3 The performance of certain functions by Local Authorities may require the directed covert surveillance of individuals or the use of informants or undercover officers, known as CHIS.

2.4 Those who undertake directed covert surveillance on behalf of a Local Authority may breach an individual's human rights, unless such surveillance is consistent with Article 8 of the ECHR and is both necessary and proportionate to the matter being investigated

2 5 As a result of the legislative changes referred to in 1 above, Local Authorities can now only authorise directed covert surveillance under RIPA for the purpose of preventing or detecting conduct which constitutes a **criminal offence** which is·

(a) punishable (whether on summary conviction or indictment) by a maximum term of at least six months imprisonment; or

(b) involves the sale of alcohol or tobacco to children

2 6 Furthermore, if authorised by an authorised officer, the Council's authorisation can only be given effect once an Order approving the authorisation has been granted by a JP

It is important to note

- A Local Authority cannot authorise the use of directed covert surveillance under RIPA to investigate low level offences e g littering, dog control and fly posting Neither can a Local Authority authorise such surveillance for the purpose of preventing disorder, unless this involves a criminal offence punishable in the way described above

- The crime threshold referred to above applies only to the authorisation of directed covert surveillance under RIPA, not to the authorisation of Local Authority use of CHIS or their acquisition of communications data

2.7 In order to properly regulate the use of directed covert surveillance and the use of CHISs in compliance with the HRA, the Regulation of Investigatory Powers Act 2000 (RIPA) came into force on 25th September 2000

2 8 RIPA requires that all applications to undertake directed covert surveillance of individuals or to use CHISs are properly authorised, recorded and monitored. The detailed procedure for undertaking directed covert surveillance or using a CHIS are set out in Parts 2 and 3

2.9 Failure to comply with RIPA may leave the Council open to potential claims for damages or infringement of individual's human rights. It may also mean that any evidence obtained in breach of the provisions of RIPA is rendered inadmissible in Court

3. What is Surveillance?

3.1 Surveillance is

- Monitoring, observing or listening to persons, their movements, their conversations or their other activities or communications

- Recording anything monitored, observed or listened to in the course of surveillance, with or without the assistance of a device.

3 2 By its very nature, surveillance involves invading an individual's right to privacy. The level of privacy which individuals can expect depends upon the nature of the environment they are within at the time For example, within an individual's own home or private vehicle, an individual can expect the highest level of privacy The level of expectation of privacy may reduce if the individual transfers out into public areas.

3 3 There are different types of surveillance which, depending on their nature, are either allowable or not allowable and require different degrees of authorisation and monitoring under RIPA

3 4 **Overt surveillance** is where the subject of surveillance is aware that it is taking place Overt surveillance is outside the scope of RIPA and therefore does not require authorisation The 2018 Code also provides guidance that authorisation under RIPA is not required for the following types of activity

- General observations that do not involve the systematic surveillance of an individual or a group of people
- Use of overt CCTV surveillance
- Surveillance where no private information is likely to be obtained
- Use of overt ANPR systems to monitor traffic flows or detect motoring offences
- Surveillance undertaken as an immediate response to a situation
- Review of staff usage of the internet & e-mail (but see Section ~~6~~ 7 below)
- Surveillance not on statutory grounds (see section 6 Surveillance outside of RIPA)

3.5 **Covert surveillance** is defined as "surveillance which 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" and is covered by RIPA Covert surveillance is categorised as either intrusive or directed

3.6 **Intrusive covert surveillance** is defined as covert surveillance that is carried out in relation to anything taking place on any residential premises or in any private vehicle and involves the presence of an individual on the premises or in the vehicle or is carried out by means of a surveillance device RIPA does not empower Local Authorities to authorise or undertake intrusive covert surveillance Other means of investigation should be considered

3 7 **Directed covert surveillance** is surveillance which is covert but not intrusive and undertaken.

- For the purposes of a planned specific investigation or operation,
- In such a manner as is likely to result in the obtaining of private information about a person (whether or not that person is specifically targeted for the purposes of an investigation or operation),and
- Other than by immediate response to circumstances when it would not be practical to seek authorisation, for example, noticing suspicious behaviour and continuing to observe it

3 7 1 **Private information** includes any information relating to a person's private or family life As a result, private information is capable of including any aspect of

a person's private or personal relationship with others, such as family and professional or business relationships

Note: Information which is non-private includes

- Publicly available information such as books, newspapers, journals, TV and radio broadcasts, newswires, web sites, mapping imagery, academic articles, conference proceedings, business reports, and more.
- Commercially available data where a fee may be charged, and any data which is available on request or made available at a meeting to a member of the public

3 7 2 Whilst a person may have a reduced expectation of privacy when in a public place, covert surveillance of that person's activities in public may still result in the obtaining of private information This is likely to be the case where that person has a reasonable expectation of privacy even though acting in public and where a record is being made by a public authority of that person's activities for future consideration or analysis. Surveillance of publicly accessible areas of the internet should be treated in a similar way, recognising that there may be an expectation of privacy over information which is on the internet, particularly where accessing information on social media websites (see 7 below)

3.7 3 Private information may include personal data, such as names, telephone numbers and address details. Where such information is acquired by means of directed covert surveillance of a person having a reasonable expectation of privacy, authorisation is required

3.7 4 Private life considerations are particularly likely to arise if several records are to be analysed together in order to establish, for example, a pattern of behaviour, or if one or more pieces of information (whether or not available in the public domain) are covertly (or in some cases overtly) obtained for the purpose of making a permanent record about a person or for subsequent data processing to generate further information. In such circumstances, the totality of information gleaned may constitute private information even if individual records do not. Where such conduct includes covert surveillance, a directed surveillance authorisation may be considered appropriate

3 7 5 Directed covert surveillance involves the observation of a person or persons with the intention of gathering private information to produce a detailed picture of a person's life, activities and associations

3 7 6 Directed covert surveillance does not include entry on or interference with property or wireless telegraphy but may include the use of photographic and video equipment (including the use of CCTV)

3 7 7 Directed covert surveillance is covered by RIPA and requires prior authorisation

4. What is a Covert Human Intelligence Source (CHIS)?

4 1 A CHIS is defined in section 25(7) of the RIPA as a person who establishes or maintains a personal or other relationship with another person for the covert purpose of facilitating anything that·

(a) Covertly uses such a relationship to obtain information or to provide access to any information to another person, or

b) Covertly discloses information obtained by the use of such a relationship or as a consequence of the existence of such a relationship

4 2 By virtue of section 26(9)(b) of RIPA 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

4 3 By virtue of section 26(9)(c) of RIPA a relationship is used covertly, and information obtained as above is disclosed covertly, if and only if it is used or, as the case may be, 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.

4 4 Special consideration must be given to the use of Vulnerable Individuals as a CHIS 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 unable to protect himself against significant harm or exploitation Any individual of this description, or a Juvenile as defined below, should only be authorised to act as a source in the most exceptional circumstances and only then when authorised by the Chief Executive (or, in her absence, the Deputy Chief Executive).

4.5 Special safeguards also apply to the use or conduct of Juvenile Sources; that is sources under the age of 18 years On no occasion should the use or conduct of a source under 16 years of age be authorised to give information against his parents or any person who has parental responsibility for him

4.6 Legal advice must be sought if considering using a vulnerable or juvenile CHIS.

4 7 It is not anticipated that CHISs will be used often in the normal course of Council investigatory activity. Any Council Officer considering the use of a

CHIS must first contact the Senior Responsible Officer or the Principal Legal Executive to discuss the suitability of this approach

4 8 Authorisation is not required when individuals, including members of the public, are requested to provide information pertaining to other individuals, unless they are required to form a relationship, or manipulate an existing relationship with those other individuals

4 9 Detailed procedures for the use of CHIS are set out in Part 3.

5. Procedural principles for Surveillance and use of CHIS's

5 1 Detailed procedures for undertaking directed covert surveillance are set out in Parts 2 and 3 of this Policy respectively

5 2 The conduct of surveillance which is consistent with these procedures can be undertaken with confidence that any evidence obtained will be admissible in a criminal trial, provided the conduct is authorised and is carried out in accordance with the authorisation The authorisation must be shown to be necessary on the grounds of preventing or detecting crime (see 2.5 above).

5 3 The Investigating Officer seeking authorisation for directed covert surveillance or CHIS activity and the Authorising Officer must give consideration to the following factors

- **Necessity** –Is directed covert surveillance or CHIS activity the only or best way to obtain the desired information in connection with a potential criminal offence of the types referred to in 2 5, or are other less invasive methods appropriate?

- **Proportionality** – Is the surveillance activity or CHIS activity proportional to the evidence that will be obtained and to the privacy the subject could reasonably expect? The methods used to obtain evidence should not be excessive and should be as non-invasive as it possible The surveillance should not restrict an individual's right for privacy more than is absolutely necessary

- **Collateral Intrusion** – Will the surveillance result in the observing of innocent people? If so can it be avoided or minimised?

5 4 Further Considerations

- Does the application relate to a criminal offence which has a maximum sentence of at least 6 months or relate to the sale of alcohol or tobacco to children

- Have other ways of getting the information been investigated?

- Is surveillance a reasonable approach and "not a sledge hammer to crack a nut"?

- The risk of the directed surveillance and CHIS activity must be considered and managed

- Surveillance authorisations remain valid for 3 months but must be cancelled prior to that if no longer required

- CHIS authorisations remain valid for 12 months and must be cancelled prior to that if no longer required

- Authorisations should be periodically reviewed by the Authorising Officer and the need for continued surveillance or CHIS activity ascertained; if no longer required, authorisations should be cancelled

5 5 All Council officers undertaking directed cover surveillance or wishing to use a CHIS must have received appropriate training to enable them to undertake this task

5 6 Training should be periodically arranged to ensure that sufficient Authorising Officers are available

5 7 Where directed covert surveillance or the use of a CHIS is likely to result in the obtaining of confidential information, it is imperative that legal advice should first be sought from the Senior Responsible Officer or the Principal Legal Executive. "Confidential information" includes, though is not limited to, matters subject to legal privilege, confidential personal information and confidential journalistic material Confidential personal information is information held in confidence relating to the physical or mental health or spiritual counselling concerning an individual (whether living or dead) who can be identified from it

5.8 The application for authorisation must include the following elements and the Authorising Officer must consider these, before authorising the directed covert surveillance or CHIS activity.

- full details of the reason for the directed covert surveillance or CHIS activity and the intended outcome,

- the proposed surveillance activity described as fully as possible, with the use of maps or other plans as appropriate,

- the necessity and proportionality to the potential offence consideration and whether other methods of less intrusive investigation should / have been attempted and whether they are appropriate,

- the resources to be applied and tactics and methods should also be included,

- the anticipated start date and duration of the activity, if necessary broken down over stages;

- details (including unique reference number) of any surveillance previously conducted on the individual

5 9 In addition the Authorising Officer should notify the Chief Executive of an authorisation

5 10 Services that undertake surveillance activity or use of CHISs should put in place adequate arrangements for the retention of evidence gathered. The arrangements must comply with the Criminal Procedure and Investigations Act 1996 and any other relevant guidance or procedures to ensure the integrity of the evidence

5.11 Evidence or intelligence obtained as a result of a RIPA authorisation should not be passed to other agencies such as the Police unless the request meets the Data Protection Act 2018 ("DPA") requirements under the Law Enforcement processing procedures or Schedule 2, Part 1 Paragraph 2 the replacement for section 29 DPA This will assist with oversight of the process

5 12 The Authorising Officer's statement on the authorisation form should clearly demonstrate agreement that the activity is necessary and proportionate and that he / she has thoroughly considered the matter before authorising and state exactly what activity is authorised, against whom, where and in what circumstances

5 13 The responsibilities of the Senior Responsible Officer are

- Maintaining the Council's RIPA Policy and Procedures

- Ensuring the integrity of the processes in place within the Council to authorise directed covert surveillance

- compliance with the legislation and Codes of Practice

- engagement with the IPCO and inspectors when they conduct their inspections,

- where necessary, overseeing the implementation of any post inspection action plans recommended or approved by the IPCO, and

- for ensuring that all *Authorising Officers* are of an appropriate standard in light of any recommendations in the inspection reports prepared by the IPCO. Where an inspection report highlights concerns about the standards of A*uthorising Officers*, this individual will be responsible for ensuring the concerns are addressed

5 14 The Principal Legal Executive will maintain a Central Record of RIPA Applications and Authorisations (including the JP approval form) This Central Record will be used to track the progress of authorisations and ensure that reviews, renewals and cancellations take place within the prescribed timeframe. Copies of all RIPA authorisations, reviews, renewals and cancellations should be forwarded to the Principal Legal Executive promptly The record will be available to the IPCO, at any time The Central Register format will be consistent with that detailed in the 2018 Code

5.15 A report on the use of RIPA will be submitted annually to the Cabinet Cabinet will consider this Policy and review the Council's use of RIPA

5 16 The head of each section which undertakes directed surveillance or CHIS activity will ensure that.

- staff receive the necessary training,
- all activity is in accordance with RIPA and the 2018 Code, and
- relevant procedures are maintained to ensure the above

6. Surveillance outside of RIPA

6.1 As a result of the change in the law from the 1st November 2012 directed covert surveillance under RIPA will only apply to the detection and prevention of a criminal offence that attracts a penalty of 6 months imprisonment or more or relates to the sale of alcohol or tobacco to children This essentially excludes surveillance of many offences that the Council may investigate such as disorder (unless it has 6 months custodial sentence) and most summary offences such as littering, dog fouling etc Other examples are referred to in 6 4 below

6 2 This change does not mean that Council enforcement officers cannot undertake such surveillance, but because it is **not** regulated by the IPCO, responsibility for monitoring this type of activity falls to the Council's Senior Responsible Officer (SRO) As a result procedures need to be in place to ensure that the Council can prove that it has given due consideration to necessity and proportionality which are central tenets of European Law and the likely grounds of any challenge

6.3 If it is necessary for the Council to undertake surveillance which does not meet the criteria to use the RIPA legislation, (such as in cases of disciplinary investigations against staff or surveillance relating to Anti-Social Behaviour appertaining to disorder) the Council must still meet its obligations under the Human Rights Act and be able to demonstrate that its actions (which may infringe a person's Article 8 rights to privacy) are necessary and proportionate, which includes taking account of the intrusion issues. To demonstrate this accountability, the decision making process and the

management of such surveillance must be documented Therefore, should Council officers need to undertake such surveillance outside of RIPA, they should complete the Non RIPA Surveillance form (available from the RIPA pages on the intranet) This should be submitted to one of the Authorising Officers listed within this Policy to be considered for authorisation before any activity can be undertaken. There will be no requirement to have the authorisation approved by a Justice of the Peace Should the activity be approved, the procedures to be followed will be the same as any RIPA authorised activity Therefore, the Council expects that the procedure and management of the activity, from the initial surveillance assessment, through to completion and cancellation to be managed appropriately at the same level that the RIPA legislation and guidance requires For further advice, refer to the RIPA pages on the Intranet.

6 4 Examples of Surveillance outside of RIPA

6 4 1 Planning

Some planning scenarios require evidence to be gathered either before service of a Notice or post service of a Notice to establish whether the Notice has been breached. A common example may be some someone running a car repair business from home. It is often the case that this causes disruption and disturbance to neighbours who complain. Diary sheets may be issued to establish the level of activity and the person may be spoken to by a Planning Enforcement officer It is often the case that the person states they only repair a few cars as a hobby for friends and family and are not running a business. At some stage it may be necessary for a Notice to be issued to the person The repairs may then continue with the neighbours complaining. It is at this stage that targeted covert surveillance may be required as the best means of gathering the required information to establish if the Notice has been breached which would be a criminal offence The offence does not meet the 6 months imprisonment criteria for it to be RIPA surveillance.

6 4.2 Social Services

Social Services need to carry out investigations to protect vulnerable persons such as children. These would not be treated as criminal investigations and are normally dealt with by the Family Court There may be occasions where some form of targeted covert surveillance activity is required to gather evidence for decision making or court proceedings. It is often the case that this type of surveillance is carried out by outside contractors. If this is the case, the above procedure for surveillance outside of RIPA should be followed in order to demonstrate that the Council has considered the activity with regard to Necessity and Proportionality and taken account of the intrusion on anyone.

6.4 3 Disciplinary Investigations

There may be serious disciplinary investigations that require some form of targeted covert surveillance activity which will engage Article 8 rights to privacy There is specific guidance issued by the Information Commissioners Office (ICO) in the Employment Practices Code under Part 3 Monitoring at

Work. There is a link to this guidance below This guidance make it clear that surveillance should only be used for serious matters and that the activity must be Necessary and Proportionate taking account of the intrusion issues.

https //ico.org uk/media/for-organisations/documents/1064/the_employment_practices_code pdf

6 4 4 In the above scenarios, if these issues were criminal investigations and the offences carried the required sentence of 6 months imprisonment they would be meet the Directed Covert Surveillance criteria under RIPA and would require authorisation However these scenarios are to be treated as targeted surveillance operations outside of RIPA and the procedure for surveillance outside of RIPA should be followed in order to demonstrate that the Council has considered the activity with regard to Necessity and Proportionality and taken account of the intrusion on anyone

6.5 Other routine activity that may be surveillance

6 5.1 There are other routine scenarios that may amount to surveillance for example the **deployment of a noise recording machine,** which may be monitoring persons and conversations etc. In these instances, the persons responsible for the noise are notified that the recording activity may take place, which would give them a reduced expectancy of privacy However, the Council still has an obligation to consider the intrusion issues and Necessity and Proportionality which will include the management and disposal of any personal data obtained Therefore, staff should carry out some form of privacy impact assessment and be able to demonstrate why it was necessary to deploy the noise machine and that it was a proportionate response to the problem to be resolved It is likely that this can be documented and managed within the case notes of that particular complaint

7 Internet and Social Media - use for Research and Investigations

7 1 Online open source research is widely regarded as the collection, evaluation and analysis of material from online sources available to the public, whether by payment or otherwise to use as intelligence and evidence

7 2 The use of online open source internet and social media research techniques has become a productive method of obtaining information concerning individuals to assist the Council with its regulatory and enforcement functions It can also assist with service delivery issues, employment matters and debt recovery However, the use of the internet and social media is constantly evolving and there are risks associated with these types of enquiries, regarding breaches of privacy under Article 8 Human Rights Act (HRA) and other operational risks

7 3 The activity may require RIPA authorisations for Directed Covert Surveillance or CHIS. Where this is the case, the application process and the contents of this Policy is to be followed

7 4 Where the activity falls within the criteria of surveillance outside of RIPA, again this will require authorising on a non RIPA form which will be authorised internally

7.5 In carrying out online research and investigations in respect of individuals regard should be had to the 2018 Code Attached at Appendix 3 is the summary of the key points relating to social media from the 2018 Code In addition the Council has prepared a separate procedure note specifically dealing with the use of the Internet and Social Media for investigations

8. Use of CCTV

8 1 The use of the CCTV systems operated by the Council do not normally fall under RIPA However, it does fall under the Data Protection Act 2018 and the Council's CCTV Policy. Guidance on operation of CCTV is provided in the "Surveillance Camera Code of Practice" issued under the Protection of Freedoms Act 2012 ("the 2012 Act") and overseen by the Surveillance Camera Commissioner Local Authorities should also be aware of the relevant Information Commissioner's code of practice ("In the Picture – A Data Protection Code of Practice for Surveillance Cameras and Personal Information") Should there be a requirement for the CCTV cameras to be used for a specific operation to conduct surveillance it is likely that the activity will fall under directed covert surveillance and therefore require an authorisation

8 2 On the occasions when the CCTV cameras are used for directed covert surveillance, either by enforcement officers from relevant departments within the Council or outside Law Enforcement Agencies such as the Police, either the CCTV staff are to have a copy of the application form in a redacted format, or at least a copy of the authorisation page. It is important that the staff check the authority and only carry out what is authorised

8 3 Operators of the Council's CCTV system need to be aware of the RIPA issues associated with using CCTV and that continued, prolonged, systematic surveillance of an individual may require an authorisation

9 Use of material as evidence

9 1 Material obtained through directed covert surveillance, may be used as evidence in criminal proceedings The admissibility of evidence is governed primarily by the common law, the Criminal Procedure and Investigations Act 1996, the Civil Procedure Rules, section 78 of the Police and Criminal Evidence Act 1984 and the Human Rights Act 1998.

9.2 Ensuring the continuity and integrity of evidence is critical to every prosecution Accordingly, considerations as to evidential integrity are an important part of the disclosure regime under the Criminal Procedure and

Investigations Act 1996 and these considerations will apply to any material acquired through directed covert surveillance or property interference that is used in evidence When information obtained under a directed covert surveillance authorisation is used evidentially, it will be necessary to be able to demonstrate how the evidence has been obtained, to the extent required by the relevant rules of evidence and disclosure

10 Safeguards of Material

10 1 The Council and all staff should ensure that their actions when handling information obtained by means of directed covert surveillance comply with the Data Protection Act 2018, General Data Protection Regulation and the Council's Data Retention Policy and the Criminal Procedures Investigations Act 1996 (CPIA) This will ensure that any interference with privacy is justified in accordance with Article 8(2) of the European Convention on Human Rights Compliance with these legal frameworks will ensure that the handling of private information so obtained continues to be lawful, justified and strictly controlled, and is subject to robust and effective safeguards

10 2 Dissemination, copying and retention of material must be limited to the minimum necessary for authorised purposes. This obligation applies equally to disclosure to additional persons within the Council and to disclosure outside the authority

10 3 Material obtained through directed covert surveillance or property interference, and all copies, extracts and summaries of it, must be handled and stored securely, so as to minimise risk It must be held so as to be inaccessible to persons who would not need to see it (where applicable). This requirement applies to all those who are responsible for the handling of the material

10 4 Any breaches of data protection requirements should be reported to the Councils DPA Officer and the SRO as it is likely to constitute an error

11 Errors

11 1 Proper application of the surveillance provisions in the 2018 Codes should reduce the scope for making errors

11 2 An error must be reported if it is a "relevant error" A relevant error is any error by a public authority in complying with any requirements that are imposed on it by any enactment which are subject to review by a Judicial Commissioner This would include compliance by public authorities with Part II of the 2000 Act (RIPA).

11 3 Examples of relevant errors occurring would include circumstances where

- Surveillance activity has taken place without lawful authorisation.

- There has been a failure to adhere to the safeguards set out in the relevant statutory provisions and Chapter 9 of the 2018 Code relating to the safeguards of the material

11.4 Errors can have very significant consequences on an affected individual's rights All relevant errors made by public authorities must be reported to the IPCO by the public authority that is aware of the error as soon as reasonably practicable and a full report no later than ten working days The report should include information on the cause of the error, the amount of surveillance or property interference conducted, and material obtained or disclosed; any unintended collateral intrusion; any analysis or action taken; whether any material has been retained or destroyed, and a summary of the steps taken to prevent recurrence.

Serious Errors

11 5 The IPCO must inform a person of any relevant error relating to that person if the Commissioner considers that the error is a serious error and that it is in the public interest for the person concerned to be informed of the error The Commissioner may not decide that an error is a serious error unless they consider that the error has caused significant prejudice or harm to the person concerned The fact that there has been a breach of a person's Convention rights (within the meaning of the Human Rights Act 1998) is not sufficient by itself for an error to be a serious error.

11 6 It is important that all staff involved in the RIPA process report any issues so they can be assessed as to whether it constitutes an error which requires reporting

12 Complaints

12.1 The Investigatory Powers Tribunal (IPT) has jurisdiction to investigate and determine complaints against Local authority use of investigatory powers, including those covered by the 2018 Code, and is the only appropriate tribunal for human rights claims against the intelligence services Any complaints about the use of powers as described in the 2018 Code should be directed to the IPT

12 2 The IPT is entirely independent from Her Majesty's Government and all public authorities who use investigatory powers It is made up of members of the judiciary and senior members of the legal profession Following receipt of a complaint or claim from a person, the IPT can undertake its own enquiries and investigations and can demand access to all information necessary to establish the facts of a claim and to reach a determination. A 'person' for

these purposes includes an organisation, an association, or combination of persons (see section 81(1) of RIPA), as well as an individual.

12 3 Further information on the exercise of the Tribunal's functions and details of the relevant complaints procedure can be obtained from

Investigatory Powers Tribunal
PO Box 33220
London
SW1H 9ZQ

Tel 0207 0353711

www ipt-uk com.

12.4. Notwithstanding the above, members of the public will still be able to avail themselves of the Council's internal complaints procedure, where appropriate, and can complain to the Local Government Ombudsman.

13 Oversight by the IPCO

13 1 The Investigatory Powers Act 2016 provides for an Investigatory Powers Commissioner ("the Commissioner"), whose remit includes providing comprehensive oversight of the use of the powers to which this Policy applies, and adherence to the practices and processes described in it The Commissioner will be, or will have been, a member of the senior judiciary and will be entirely independent of Her Majesty's Government or any of the public authorities authorised to use investigatory powers The Commissioner will be supported by inspectors and others, such as technical experts, qualified to assist the Commissioner in his or her work The Commissioner will also be advised by the 'Technology Advisory Panel'

13 2 One of the duties of the IPCO is to carry out planned inspections of those public authorities who carry out surveillance as specified in RIPA, to ensure compliance with the statutory authorisation procedures At these inspections they have unfettered access to all locations, documentation and information systems as necessary to carry out their full functions and duties All relevant persons using investigatory powers must provide all necessary assistance to the Commissioner and anyone who is acting on behalf of the Commissioner

13 3 An inspection report will be presented to the Chief Executive, which should highlight any significant issues, draw conclusions and make appropriate recommendations The aim of inspections is to be helpful rather than to measure or assess operational performance

13 4 In addition to routine inspections, spot checks may be carried out from time to time.

13 5 There is a duty on every person who uses the powers provided by Part II of RIPA, which governs the use of directed covert surveillance or covert human intelligence sources, to disclose or provide to the Chief Commissioner (or his duly appointed Inspectors) all such documents and information that he may require for the purposes of enabling him to carry out his functions

PART 2

DETAILED PROCEDURES FOR UNDERTAKING DIRECTED COVERT SURVEILLANCE

1. **Purpose**

To ensure that surveillance is only undertaken in appropriate cases, is properly authorised and recorded and is compliant with the Human Rights Act 1998, the Regulation of Investigatory Powers Act 2000 and appropriate Code of Practices, made there under

2 **Scope**

2 1 These procedures must be complied with by all sections and Investigating Officers, who routinely or occasionally undertake directed covert surveillance in connection with preventing or detecting crime with a maximum 6 months imprisonment or relate to the sale of alcohol or tobacco to children (the only permitted purpose for such surveillance). Local investigation procedures should make reference to this Policy

3. Procedure

3 1 It is very important that the correct authorisation procedure is followed prior to undertaking surveillance activity Interference of the right to privacy without proper authorisation may render any evidence obtained unusable in a criminal court If surveillance is conducted on individuals without the necessary authorisation, the Council and possibly individuals may be sued for damages for a breach of Human Rights In civil matters adverse inferences may be drawn from such interference.

3 2 This procedure is supported by the 2018 Code. If the surveillance is not likely to obtain private information, the 2018 Code does not apply. All Investigating Officers and Authorising Officers should fully acquaint themselves with the 2018 Code and refer to it during both the application and authorisation processes

3 3 All directed covert surveillance activity must be approved prior to the activity taking place by an Authorising Officer and a Justice of the Peace ("JP") Officers seeking authority to undertake directed covert surveillance should complete the form, "Application for use of Directed Covert Surveillance" A sample application form with notes is attached at **Appendix 1**, but the latest

version from the Gov UK website must always be used. Completed application forms should be forwarded to the relevant Authorising Officer.

3.4 Completed authorisation forms should be allocated a reference number by the Investigating Officer relevant to the department / team and the particular investigation The Investigating Officer should also obtain the next unique reference number from the Central Record of RIPA Applications and Authorisations maintained by the Principal Legal Executive.

3 5 The Authorising Officer will consider the completed application form and inform the Investigating Officer of his / her decision The Authorising Officer will retain a copy of the authorisation form and monitor this for review, renewal and cancellation should it be approved by a JP The original will be required to be returned to the applicant if authorised to be presented before a JP If refused by the Authorising Officer or JP the original will be forwarded to the Principal Legal Executive for filing.

3.6 In addition the Authorising Officer must notify the Chief Executive of an authorisation

3 7 The Investigating Officer and the Authorising Officer must give consideration to the following factors.

- **Necessity** – is covert surveillance the only or best way to achieve the desired information, or are other less invasive methods appropriate?
- **Proportionality:**
    - balancing the size and scope of the proposed activity against the gravity and extent of the perceived crime or offence,
    - explaining how and why the methods to be adopted will cause the least possible intrusion on the subject and others,
    - considering whether the activity is an appropriate use of the legislation and a reasonable way, having considered all reasonable alternatives, of obtaining the necessary result; and
    - evidencing, as far as reasonable practicable, what other methods had been considered and why they were not implemented
- **Collateral intrusion** – that is the obtaining of information relating to persons other than the subject of the investigation and the need to minimise this.
- **Confidential Information** - The Investigating Officer and the Authorising Officer must consider the possibility that the surveillance activity may result in the acquiring of confidential information. If this is

considered to be likely then the Investigating Officer must highlight this on the application

3.8 All Investigating Officers completing RIPA applications must ensure that applications are sufficiently detailed When completing an application or authorisation, the Investigating Officer and Authorising Officer must ensure that the case for the authorisation is presented in the application in a fair and balanced way In particular, all reasonable efforts should be made to take into account information which weakens the case for the warrant or authorisation Authorising Officers should refuse to authorise applications that are not to the required standard and should refer them back to the Investigating Officers

3.9 **Magistrates' Court Approval:** As from the 1st November 2012 all applications and renewals for Directed Covert Surveillance and use of a CHIS will be required to have a JP's approval

3.10 Having had the activity authorised by the Authorising Officer, the Investigating Officer must now complete the relevant Judicial Approval form to seek approval from a JP. The Investigating Officer must ensure compliance with the statutory provisions and should refer to the Home Office publication (October 2012) "Protection of Freedoms Act 2012 – changes to provisions under the Regulation of Investigatory Powers Act 2000 (RIPA) Home Office guidance to local authorities in England and Wales on the judicial approval process for RIPA and the crime threshold for directed surveillance"

https://www gov uk/government/publications/changes-to-local-authority-use-of-ripa)

3.11 The Judicial Approval form (see **Appendix 2**) will be submitted to the JP for approval The form requires the Investigating Officer to provide a brief summary of the circumstances of the case on the judicial application form

3 12 The contact numbers for Her Majesty's Court and Tribunals Service to arrange a hearing is

- Within office hours 01245 313315 or 01245 313313
- If out of hours the contact numbers are 07736 638551 or 07774 238418

3 13 At the hearing which is on oath, the officer must present to the JP.

- the partially completed judicial approval/ order form,
- a copy of the RIPA application / authorisation form, together with any supporting documents setting out the case, and

- the original application / authorisation form (this must be retained by Investigating Officer)

It is preferred that the Authorising Officer also attends the hearing at the Magistrates' Court

3.14 The JP will consider the paperwork and may ask questions to clarify points or require additional reassurance on particular matters

The JP will

- Consider whether he or she is satisfied that at the time the authorisation was granted or renewed, there were reasonable grounds for believing that the authorisation was necessary and proportionate,
- Consider whether there continues to be reasonable grounds;
- Consider whether the person who granted the authorisation or gave the notice was an appropriate designated person within the Local Authority, and
- Consider whether if the authorisation was made in accordance with the law, i.e. that the crime threshold for directed covert surveillance has been met

3 15 The JP may:

- Decide to approve the Grant or renewal of an authorisation which will then take effect and the Local Authority may proceed to use the technique in that particular case, or
- Refuse to approve the grant or renewal of an authorisation in which case the RIPA authorisation will not take effect and the Local Authority may not use the technique in that case

3 16 Where an application has been refused the Investigating Officer should consider the reasons for that refusal. If more information was required by the JP to determine whether the application / authorisation has met the tests, and this is the reason for refusal, the Investigating Officer should consider whether they can reapply, for example, if there was information to support the application which was available to the Local Authority, but not included in the papers provided at the hearing.

3 17 Where the JP refuses to approve the application / authorisation or renew the application / authorisation and decides to quash the original authorisation or notice the court must not exercise its power to quash the application / authorisation unless the applicant has had at least 2 business days from the date of the refusal in which to make representations If this is the case the officer will inform Legal Services who will consider whether to make any representations.

3 18 Whatever the decision, the JP will record their decision on the order section of the judicial application / order form The court will retain the copy of the Local Authority RIPA application and authorisation form and the judicial application / order form. The officer will retain the original application / authorisation and a copy of the judicial application / order form

3 19 As previously stated the Principal Legal Executive is responsible for giving each authorisation a central unique identification number using a standard consistent format and recording it in a Central Record of RIPA Applications and Authorisations. This is to ensure that an up-to-date central record is maintained for all directed covert surveillance activity Similarly, copies of all cancellations, renewals and review applications should be forwarded to the Principal Legal Executive promptly. The original authorisation should be kept on the investigation file

3 20 Written surveillance authorisations last for a maximum of three months. They cannot be authorised for a lesser period and the commencement date is the date approved by the J P Surveillance authorisations must be cancelled when no longer required (see 3 30 below)

Reviews

3 21 The Authorising Officer has the responsibility to set the review dates for each authorisation and will determine what the review dates will be. The review date is detailed on the authorisation form. The review date will be at most one month from the date approved by the JP or previous review. The Authorising Officer should conduct the review with the Investigating Officer Reviews should not be conducted solely by the Investigating Officer Details of the review should be recorded on the form "Review of the use of Directed Surveillance Authorisation", available on the Home Office website and retained with the original authorisation. The Authorising Officer must ensure through diarisation or otherwise that reviews are conducted at the correct date

3 22 Any proposed or unforeseen changes to the nature or extent of the surveillance operation which may result in the further or greater intrusion into the private life of any person should be brought to the attention of the Authorising Officer by means of a review.

3 23 There is no requirement for a review form to be submitted to a JP. However if a different surveillance techniques is required it is likely a new application will have to be completed and approved by a JP.

Renewal

3.24 Should it be necessary to renew a Directed Covert Surveillance or CHIS application / authorisation, this must be approved by a JP

3 25 Applications for renewals should not be made until shortly before the original authorisation period is due to expire but the applicant must take account of factors which may delay the renewal process (e g. intervening weekends or the availability of the relevant authorising officer and a JP to consider the application)

3 26 The applicant should complete all the sections within the renewal form and submit the form to the Authorising Officer

3 27 Authorising Officers should examine the circumstances with regard to Necessity, Proportionality and the Collateral Intrusions issues before making a decision to renew the activity A CHIS application should not be renewed unless a thorough review has been carried out covering the use made of the source, the tasks given to them and information obtained The Authorising Officer must consider the results of the review when deciding whether to renew or not The review and the consideration must be documented

3 28 If the Authorising Officer refuses to renew the application the cancellation process should be completed If the Authorisation Officer authorises the renewal of the activity the same process is to be followed as mentioned earlier for the initial application

A renewal takes effect on the day on which the authorisation would have ceased and lasts for a further period of three months.

Cancellation

3 29 The Investigating Officer must complete the "Cancellation of the use of Directed Covert Surveillance" form available on the Home Office website and forward to the Authorising Officer who granted or last renewed the authorisation It must be cancelled if they are satisfied that the directed covert surveillance no longer meets the criteria upon which it was authorised Where the Authorising Officer is no longer available, this duty will fall on the person who has taken over the role of Authorising Officer or the person who is acting as Authorising Officer

3 30 As soon as the decision is taken that directed covert surveillance should be discontinued, the applicant or other investigating officer involved in the investigation should inform the Authorising Officer. The Authorising Officer will formally instruct the Investigating Officer to cease the surveillance, noting the time and date of their decision This will be required for the cancellation form. The date and time when such an instruction was given should also be recorded in the Central Record of RIPA Applications and Authorisations along with a note of the amount of time spent on the surveillance

3 31 The officer submitting the cancellation must complete in detail the relevant sections of the form and include the period of surveillance and if any images were obtained and any images containing third parties The Authorising

Officer must then take this into account and issues instructions regarding the management and disposal of the images etc

3 32 The cancellation process should also be used to evaluate whether the objectives have been achieved and whether the applicant carried out what they stated was necessary in the application form. This check will form part of the oversight function. Where issues are identified they will be brought to the attention of the line manager and the Senior Responsible Officer This will assist with future audits and oversight

4. Joint Agency Surveillance

4 1 In cases where one agency is acting on behalf of another, it is usually for the lead agency to obtain or provide the authorisation subject to 4 2 below. For example, where surveillance is carried out by Council employees on behalf of the Police, authorisation would be sought by the Police. If it is a joint operation involving both agencies the lead agency should seek authorisation Council staff involved with joint agency surveillance are to ensure that all parties taking part are authorised on the authorisation page of the application to carry out the activity and at all times their line manager must be made aware of the joint surveillance When Council staff are operating on another organisation's authorisation they should obtain either a copy of the application form (redacted if necessary) or a copy of the authorisation, containing the unique number This will ensure they see what activity they are authorised to carry out They should also inform the Senior Responsible Officer or the Principal Legal Executive of the unique reference number, the agencies involved and the name of the officer in charge of the surveillance.

Commissioned Services

4 2 If the Council commissions another Local Authority to undertake investigatory services on its behalf and directed covert surveillance or the use of a CHIS is required, then that other Local Authority will normally obtain the necessary authorisation under its RIPA procedures including making application to the Magistrates' Court. The other Local Authority must supply the Council with a copy of the authorisation form.

PART 3
DETAILED PROCEDURES FOR USE OF COVERT HUMAN INTELLIGENCE SOURCES (CHIS)

1 1 RIPA covers the activities of Covert Human Intelligence Sources (CHIS) which relates not only to sources commonly known as informants (members of the public providing the Council with information), but also the activities of undercover officers It matters not whether they are employees of the Council, agents or members of the public engaged by the Council to establish or maintain a covert relationship with someone to obtain information However, not all human intelligence source activity will meet the definition of a CHIS. For example, a source may be a public volunteer or someone who discloses information out of professional or statutory duty or has been tasked to obtain information other than by way of a covert relationship

1 2 Recognising when a source becomes a CHIS is important as this type of activity may need authorisation

1 3 There is a separate CHIS Policy which provides advice as to when someone is a CHIS and requires authorisation under RIPA together with the requirements involved in the process

1 4 Should a CHIS authority be required, all of the staff involved in the process should make themselves fully aware of all of the CHIS Codes of Practice.

1 5 Legal advice should always be sought where consideration is given to the use of CHIS.

Appendix 1(a)

RIPA FLOW CHART 1 : DIRECTED SURVEILLANCE

Requesting Officer (The Applicant) must

Read the Corporate Policy & Procedures Document and be aware of any other guidance

Determine that directed surveillance is required (For CHIS see Flowchart 2)

Assess whether authorisation will be in accordance with the law

Assess whether authorisation is necessary under RIPA and whether it could be done overtly

Consider whether surveillance will be proportionate

If authorisation is approved review or renew regularly with Authorised Officer

If a less intrusive option is available and practicable USE THAT OPTION! use that option

If authorisation is necessary and proportionate, prepare and submit your application form to the Authorised Officer

Authorised Officer must

- Consider in detail whether all options have been duly considered, including the Corporate Policy & Procedures Document and any other guidance issued by the SRO
- Consider whether surveillance is considered by him/her to be in accordance with the law, necessary and proportionate
- Authorise only if an overt or less intrusive option is not practicable

The Applicant must **REVIEW REGULARLY** And complete the review form and submit to Authorised

The Applicant must If operation is no longer necessary or proportionate, complete **CANCELLATION FORM** and submit to Authorised Officer

Essential Applications for Directed Surveillance will be completed on the electronic database and need to be maintained appropriately The electronic database forms the Central Database for RIPA

Authorised Officer must. If surveillance is still necessary and proportionate after authorised period

- Renew authorisation
- Set an appropriate further review date and use

Authorised Officer must: Cancel authorisation when it is no longer necessary or proportionate to need the same

NB if in doubt, ask the Group Manager (Legal and Democratic) BEFORE any directed surveillance and/or CHIS is authorised, reviewed, renewed, cancelled, or rejected.

Appendix 1 *(b)*

SAMPLE APPLICATION FORM FOR USE OF DIRECTED COVERT SURVEILLANCE

Unique Reference Number	Refer to your policy as to how you obtain the unique number. All applications must have one and put on each page.

Part II of the Regulation of Investigatory Powers Act 2000

Authorisation Directed Surveillance

Public Authority *(including full address)*	State your Public Authority Name and full address		
Name of Applicant	Details of the person completing the form	**Unit/Branch /Division**	Section and department
Full Address	Provide the address of your department		
Contact Details	Provide full contact details including email address. Make it easy for the Authorising Officer, or anyone else associated with the process to contact you.		
Investigation/Operation Name (if applicable)	This may be an investigation reference number allocated to this case, or some other reference		
Investigating Officer (if a person other than the applicant)	If the form is being completed by someone who is not the investigator, then the investigators details must be put in this box.		

DETAILS OF APPLICATION
1. Give rank or position of authorising officer in accordance with the Regulation of Investigatory Powers (Directed Surveillance and Covert Human Intelligence Sources) Order 2010 No. 521. [1]
As above. **For local authorities: The exact position of the authorising officer should be given. For example, Head of Trading Standards.** **Also use the description of the person's position contained within your policy to remove any confusion.**
2. Describe the purpose of the specific operation or investigation.
Describe the investigation to date including the offences and the relevant legislation. When, where and how are the offences occurring. Remember the Authorising Officer needs to be clear what the offence is and the circumstances. (keep information relevant and to the point) **Include the details of the suspects and persons involved and the role they play within the investigation. (Do not put confidential information in such as informants' names)** **Consider disclosure implications under CPIA with regards to not revealing unnecessary information. However, the AO needs sufficient relevant information to make a decision. The provisions of using CPIA sensitive information may be a way of dealing with the sensitivity issues later, by editing material if it has to be disclosed. However, if the document contains sensitive information remember to keep it secure at all times.** **Cross reference where necessary to other relevant applications**
3. Describe in detail the surveillance operation to be authorised and expected duration, including any premises, vehicles or equipment (e.g. camera, binoculars, recorder) that may be used.
This should be completed, after attending the area of where the activity is to be carried out, and having carried out a surveillance assessment having taken into account risks or limiting factors. Limiting factors are anything can affect the success of the operation. **Consider the AO statement in box 12, the 5 WH. The applicant can only do what is authorised by the AO, not what they have applied for.** **Consider the aims and objectives, confirmation of address may only need static observations; however, lifestyle intelligence may require foot/mobile and use of covert cameras etc.** **What exactly do you want to do? Is it static observations, foot or mobile? You want a combination? However, only ask for what you can realistically carry out. It is not a wish list; it should be carried out to achieve the objectives.** **How do you want to carry out the surveillance and what equipment do you want to use? You must make the AO aware of the capabilities of any equipment you want to use.**

[1] For local authorities. The exact position of the authorising officer should be given. For example, Head of Trading Standards

Where is the activity to take place? Who is the activity against and when do you want to carry it out?

What is the expected duration? It does not mean that it must only be authorised to this point. Once signed, the authorisation lasts for a 3 month period. You must update the AO when they set the review dates. If your operation ends prior to any review date or the 3 month period, you must cancel it straight away and submit the cancellation form. It does not expire.

REMEMBER YOU CAN ONLY DO WHAT IS AUTHORISED ON THE AO SECTION, NOT WHAT YOU HAVE APPLIED FOR IN THIS SECTION.

4. The identities, where known, of those to be subject of the directed surveillance.

- Name:
- Address:
- DOB:
- Other information as appropriate:

If you do not know who the subjects are, insert any descriptions you may have. If as a result of the surveillance, you identify anyone, you must submit this information on a review form to the AO.

Consider any known associates. If the intelligence is that the subject of the surveillance has known associates, are they likely to become subjects of the surveillance? If so, detail them as part of the application.

5. Explain the information that it is desired to obtain as a result of the directed surveillance.

These are the surveillance objectives. They should have been identified during the planning stage and a feasibility study carried out to assess whether they can be achieved. It's no use setting objectives that can't be achieved.

What is the surveillance going to tell you?

What, if any, criminality will it establish?

Will it identify subjects involved in criminality?

Will it house subject or their criminal associates?

E.G.

- Identify the location of the subject's place of work
- To gather intelligence and evidence to establish the extent of the criminality (size).
- Identify other persons involved, such as suppliers.
- Identify other premises involved, such as storage buildings.
- Obtain best evidence through the use of photographic equipment to assist with identifying the offenders
-

Obtain best evidence to assist with a prosecution of offenders

6. Identify on which grounds the directed surveillance is <u>necessary</u> under Section 28(3) of RIPA. *Delete those that are inapplicable. Ensure that you know which of these grounds you are entitled to rely on (SI 2010 No.521).*

- In the interests of national security;

- For the purpose of preventing or detecting crime or of preventing disorder;
- In the interests of the economic well-being of the United Kingdom;
- In the interests of public safety;
- For the purpose of protecting public health;
- For the purpose of assessing or collecting any tax, duty, levy or other imposition, contribution or charge payable to a government department;

For Directed Surveillance, Local Authorities only lawful purpose is preventing or detecting crime and the crime must be capable of carrying six months imprisonment or criminal offences relating to the underage sale of alcohol or tobacco under sections 146, 147 or 147A of the Licensing Act 2003 or section 7 of the Children and Young Persons Act 1933.

Due to the nature of the offences, if any other areas above are applicable such as protection of public health, this should be made clear in the body of the application and the proportionality section.

7. Explain why this directed surveillance is necessary on the grounds you have identified [Code paragraph 3.3].

You can reiterate the criminal offences

Why is it necessary at this stage of the enquiry to carry out covert activity?

What is the purpose of the operation?

How will the activity assist or progress the investigation?

What will be the consequences of the proposed action be to the victim?

Why do we need this evidence/intelligence/information?

What other enquiries have been carried out and results? This does not have to be a last resort, but if there is a less intrusive way of achieving your objectives you should take that option, or explain why you can't take that option.

Consequences of not taking action

It is not for the applicant to state on the application that they believe it to be necessary. This is the responsibility of the AO to reach that decision.

8. Supply details of any potential collateral intrusion and why the intrusion is unavoidable. [Bear in mind Code paragraphs 3.8 to 3.11.]

Describe precautions you will take to minimise collateral intrusion.

There are three parts to this section (see above). You must answer them all, as this section directly impacts upon the proportionality test.

1. SUPPLY DETAILS OF POTENTIAL COLLATERAL INTRUSION

Visit the location of where the activity is to take place and carry out a risk assessment. Who lives at the property that you may be watching. Have they got children who might be affected such as going to school etc.?

Determine where you need to be to carry out the surveillance. What else can you see?

What equipment will you be using and what will it see and record?

Consider Confidential Information

It may be useful to paint the picture in words of what it is you will be watching in the locality. This will assist the AO. You may also want to refer to any plans or maps attached to the application.

2. WHY IS THE INTRUSION UNAVOIDABLE?

Consider why the intrusion is unavoidable, such as the location and time frame that the observations have to be carried out. It may be that you are limited to the use of certain equipment only and therefore governed by its operating capabilities. Your observation position may be the only place you can use.

3. DESCRIBE THE PRECAUTIONS YOU WILL TAKE TO MINIMISE COLLATERAL INTRUSION

Having carried out the risk assessment and identified what the intrusion is, consider ways of reducing the intrusion, or keeping it to a minimum. You should consider:

State who the activity will be focused on, such as the subject etc., not the innocent third parties subject to the collateral intrusion.

Keeping the surveillance activity focussed with regards to length of time spent on the observations. However, remember that you still need time to achieve your objectives. You will need some flexibility built in to your timings.

If using technical equipment such as video or covert recordings, consider the position and focal length of the lenses when filming to reduce the intrusion. Consider when and who you will use the equipment against, such as the suspects only.

How will you manage any images obtained? Consider Data Protection, confidentiality, security, dissemination of the images, and any guidance provided by your organisation, including any Home Office guidance.

Are the staff trained to carry out the activity? If so, this may assist, as they should know what they are doing with regards to collateral intrusion.

The activity needs to be tightly managed and reviewed constantly. If there is a considerable change in the intrusion once the activity commences, then the AO needs to be made aware.

9.	Explain <u>why</u> this directed surveillance is proportionate to what it seeks to achieve. How intrusive might it be on the subject of surveillance or on others? And why is this intrusion outweighed by the need for surveillance in operational terms or can the evidence be obtained by any other means [Code paragraphs 3.4 to 3.7]?

In the necessity box we stated why it was necessary to carry out the covert activity. In this box we are assessing whether the actions requested are proportionate to the overall operational aims within the investigation, having taken into account of the intrusion issues.

How serious are the offences under investigation? What is the direct or accumulative consequence of the offences?

What are the effects of the offences on the victim or the consequences of what is happening?

Are you asking to do a lot to achieve a little? Do not use a sledgehammer to crack the nut. If you have provided a good explanation of how the intrusion will be reduced and managed in the collateral intrusion box, refer them to it.

Explain why you need to undertake this activity to achieve your objectives, against using other methods. Why, in operational terms, does your need to use the activity (how the activity will progress the investigation) outweigh the level of intrusion? Why is this method the least intrusive option?

Are your methods/tactics balanced in relation to the likely results?
Consider the length of time of the surveillance operation

What methods are required to achieve the objectives and are there any less intrusive methods? You should explain what if any less intrusive methods have been considered. If they can be used they should be. If however less intrusive methods cannot be used, explain why. You should also take account that technical surveillance may be more intrusive.

Consequences of not taking action.

10. Confidential information [Code paragraphs 4.1 to 4.31].
INDICATE THE LIKELIHOOD OF ACQUIRING ANY CONFIDENTIAL INFORMATION:

Is there any likelihood of Health, Solicitors, Counselling, and Spiritual etc.

It is unlikely that you will obtain this type of material, but an assessment should take place. If you are, it is a higher level of Authorising Officer who needs to consider it.

Do not mix this up with Private Information which is part of the consideration when assessing whether the activity falls under RIPA.

11. Applicant's Details

Name (print):		**Tel No:**	
Grade/Rank		**Date:**	
Signature			

12. Authorising Officer's Statement. [Spell out the "5 Ws" – Who; What; Where; When; Why and HOW– in this and the following box.]

I hereby authorise directed surveillance defined as follows [*Why is the surveillance necessary, whom is the surveillance directed against, Where and When will it take place, What surveillance activity/equipment is sanctioned, How is it to be achieved?]*

REMEMBER THAT EACH CASE HAS TO BE ASSESSED ON ITS OWN MERITS.

Who are you authorising to carry out the activity? Are the staff from one office? Or if a joint operation, please state that fact and name the other organisation. You have to actually authorise the other organisation's staff in writing.

What are you authorising them to do and what equipment are you authorising them to use? You

should have a knowledge of the equipment's capability.

Who are you authorising them to do it against, person, address, vehicle, etc?

When are you authorising them to do it?
Where are you authorising the activity to take place?
Why are you authorising whatever you are allowing them to do? They should have stated within the application earlier what they are hoping to achieve.
When authorising the activity, it is live for 3 months. In other words, as an AO, you cannot authorise for less. You should set a review date for you to review it if you think that the surveillance should be a shorter period.

DO NOT BE AFRAID AS AN AO, TO ONLY ALLOW THEM TO UNDERTAKE CERTAIN ACTIVITY, AS OPPOSED TO ALL THE ACTIVITY APPLIED FOR, IF IT MEANS THAT IT IS PROPORTIONATE. STATE WHY ON THE FORM

IF NOT AUTHORISING, STATE WHY.

13. Explain why you believe the directed surveillance is necessary [Code paragraph 3.3]. Explain why you believe the directed surveillance to be proportionate to what is sought to be achieved by carrying it out [Code paragraphs 3.4 to 3.7].

IF YOU ARE WRITING IN THIS SECTION, PRINT THE FORM OUT WITH ENOUGH SPACE TO WRITE IN. YOU WILL REQUIRE SOME SPACE TO DETAIL HOW YOU HAVE COME TO YOUR DECISION.

Below are 5 areas that should be dealt with by the AO when considering the application.

Code 3.3 requires that the person granting an authorisation BELIEVES that the authorisation is necessary in the circumstances of the particular case for one of the statutory reasons (see box 6). Have they made clear what the offence or offences are in the body of the application?

Code 3.4 then if the activities are necessary, the person granting the authorisation must BELIEVE that they are proportionate to what is sought to be achieved by carrying them out. AO must also BELIEVE that the objectives can't be met by other less intrusive means.

Sec 72 RIPA 2000, a person exercising or performing any power or duty in relation to which provision may be made by a code of practice under section 71 shall, in doing so, HAVE REGARD TO THE PROVISIONS (so far as they are applicable) of every code of practice for the time being in force under that section. (You have to know what the codes say).

Collateral Intrusion Code of Practice 3.8 before authorising surveillance the authorising officer should 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.

Code of Practice 3.15 .Any person granting or applying for an authorisation will also NEED TO BE AWARE OF particular sensitivities in the local community where the surveillance is taking place and of similar activities being undertaken by other public authorities which could impact on the deployment of surveillance.

This will take some consideration. Read and study the application fully. Refer to the applicants boxes that deal with these issues.

Detail your thought processes. How have you come to the conclusion? Do not rubber stamp, do not use template or cut and paste answers. This is your original note that you may be relying on in

court. If you are making decisions from reading supporting material, mention the material and keep a copy which needs to be part of the central register. Be careful to make your decisions on written material not discussions with the case officer which may be difficult to justify at a later date at court.

Model answer from codes and OSC

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

14	(Confidential Information Authorisation.) Supply detail demonstrating compliance with Code paragraphs 4.1 to 4.31.
This is completed by the AO who has the responsibility to consider the authorisation if confidential information is likely to be obtained. (Usually someone of a much higher position than a normal AO.) e.g. In a Local Authority it will be the Chief Executive. See rear of codes of practice for relevant position and refer to your policy.	
Date of first review	AO must set the review date. Consider what the applicant has stated regarding the length of time required. Remember, this is so you as the AO can now review the need for the activity to continue on the date you have set. Also refer to policy. Most state that it must not be longer than a month. However, you must assess it against all the facts.
Programme for subsequent reviews of this authorisation: [Code paragraph 3.23]. Only complete this box if review dates after first review are known. If not or inappropriate to set additional review dates then leave blank.	
As above.	

Name (Print)		**Grade / Rank**		
Signature		**Date and time**		
Expiry date and time [e.g.: authorisation granted on 1 April 2005 - expires on 30 June 2005, 23.59]		**From 1 Nov 12 this date will be from when a Magistrate approves it. Put in the expiry date. Remember it lasts for 3 months once signed (see opposite)**		

15 **Urgent Authorisation [Code paragraph 5.9]: Authorising officer: explain why you considered the case so urgent that an oral instead of a written authorisation was given.**

OSC guidance states that there is no longer a requirement to complete the whole application form; contemporaneous notes should have been made by both applicant and AO. However, check what your policy says as some organisations still require at least this part to be completed with certain other sections. If your policy does not make it clear, seek advice.

FROM 1 NOVEMBER 2012 THERE WILL BE NO URGENT PROVISIONA AVAILABLE FOR LOCAL AUTHORITIES

16 **If you are only entitled to act in urgent cases: explain why it was not reasonably practicable for the application to be considered by a fully qualified authorising officer.**

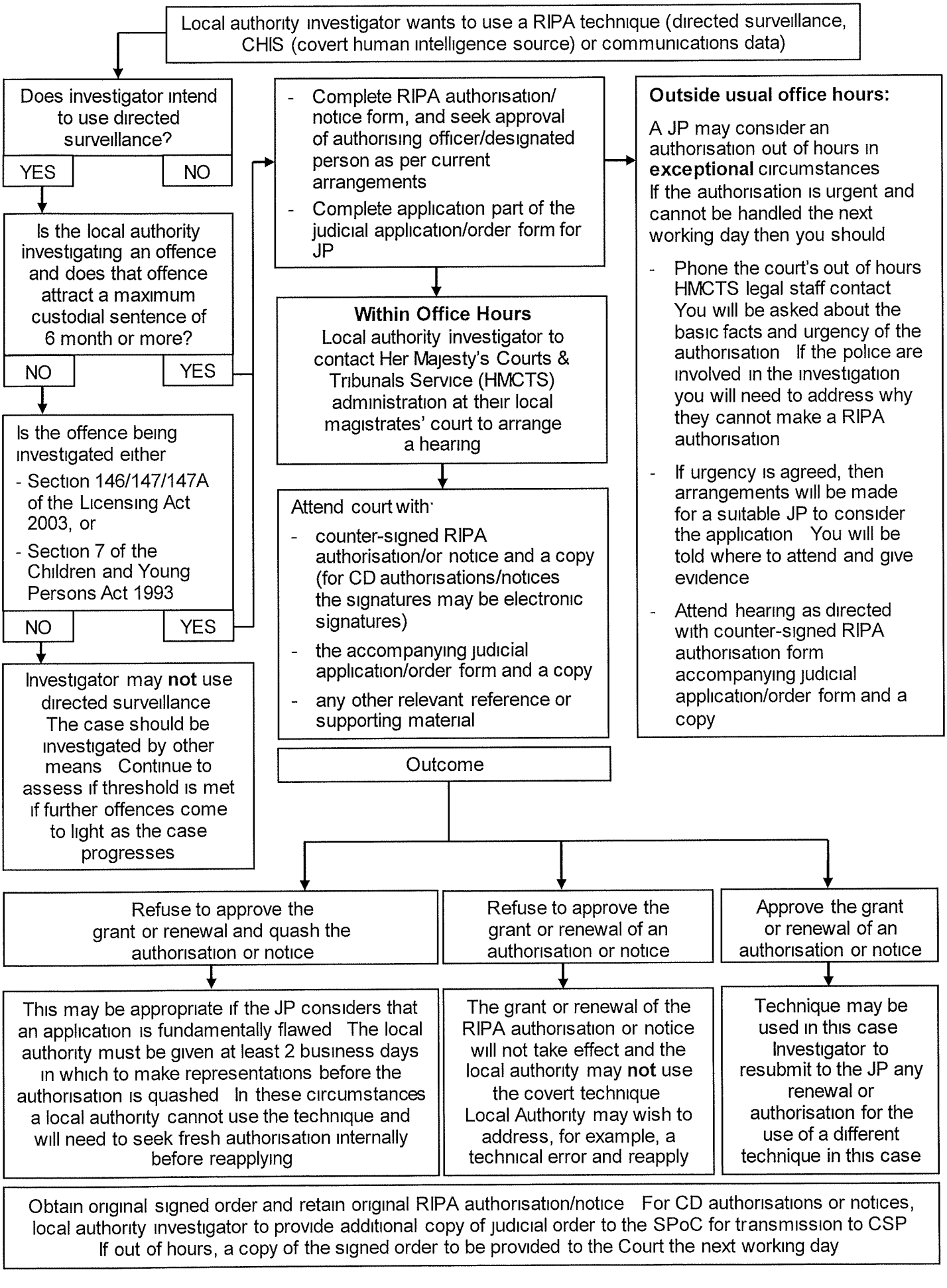
This is because the legislation allows for a lower rank/grade to authorise in urgent cases for some organisations. Refer to your policy.

See Statutory Instrument 2010 No 521.

Name (Print)		**Grade/ Rank**		
Signature		**Date and Time**		
Urgent authorisation Expiry date:		**Expiry time:**		
Remember the 72 hour rule for urgent authorities – check Code of Practice.	e g. authorisation granted at 5pm on June 1st expires 4 59pm on 4th June			

APPENDIX 2A

LOCAL AUTHORITY PROCEDURE: APPLICATION TO A JUSTICE OF THE PEACE SEEKING AN ORDER TO APPROVE THE GRANT OF A RIPA AUTHORISATION OR NOTICE



Appendix 2 *(b)*

COPY APPLICATION FORM AND ORDER FOR JUDICIAL APPROVAL

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

Local authority:

Local authority department:

Offence under investigation:

Address of premises or identity of subject

Covert technique requested: (tick one and specify details)

Communications Data	☐
Covert Human Intelligence Source	☐
Directed Surveillance	☐

Summary of details

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

Investigating Officer

Authorising Officer/Designated Person:

Officer(s) appearing before JP:

Address of applicant department:

Contact telephone number:

Contact email address (optional)

Local authority reference:

Number of pages:

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

Magistrates' court:.....

Having considered the application, I (tick one):

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

☐ refuse to approve the grant or renewal of the authorisation/notice

☐ refuse to approve the grant or renewal and quash the authorisation/notice.

Notes

.....

.....

.....

.....

.....

Reasons

.....

.....

.....

.....

.....

.....

Signed

Date:

Time:

Full name.

Address of magistrates' court:

Appendix 3

Summary of the key points relating to Social Media from the

Covert Surveillance and Property Interference Revised Code of Practice August 2018

Online Covert Activity (Directed Surveillance Codes Aug 18)

3 4 Whilst a person may have a reduced expectation of privacy when in a public place, covert surveillance of that person's activities in public may still result in the obtaining of private information. This is likely to be the case where that person has a reasonable expectation of privacy even though acting in public and where a record is being made by a public authority of that person's activities for future consideration or analysis. Surveillance of publicly accessible areas of the internet should be treated in a similar way, recognising that there may be an expectation of privacy over information which is on the internet, particularly where accessing information on social media websites. See paragraphs 3.10 to 3.17 below for further guidance about the use of the internet as a surveillance tool

3.10 The growth of the internet, and the extent of the information that is now available online, presents new opportunities for public authorities to view or gather information which may assist them in preventing or detecting crime or carrying out other statutory functions, as well as in understanding and engaging with the public they serve It is important that public authorities are able to make full and lawful use of this information for their statutory purposes. Much of it can be accessed without the need for RIPA authorisation, use of the internet prior to an investigation should not normally engage privacy considerations But if the study of an individual's online presence becomes persistent, or where material obtained from any check is to be extracted and recorded and may engage privacy considerations, RIPA authorisations may need to be considered The following guidance is intended to assist public authorities in identifying when such authorisations may be appropriate.

3.11 The internet may be used for intelligence gathering and/or as a surveillance tool. Where online monitoring or investigation is conducted covertly for the purpose of a specific investigation or operation and is likely to result in the obtaining of private information about a person or group, an authorisation for directed surveillance should be considered, as set out elsewhere in this code Where a person acting on behalf of a public authority is intending to engage with others online without disclosing his or her identity, a CHIS authorisation may be needed (paragraphs 4 10 to 4 16 of the Covert Human Intelligence Sources code of practice provide detail on where a CHIS authorisation may be available for online activity).

3.12 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, where a public authority has taken reasonable steps to inform the public or particular individuals that the surveillance is or may be taking place, the activity may be regarded as overt and a directed surveillance authorisation will not normally be available.

3 13 As set out in paragraph 3.14 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.

3 14 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.

3.15 Whether a public authority interferes with a person's private life includes a consideration of the nature of the public authority's activity in relation to that information. Simple reconnaissance of such sites (i.e. preliminary examination with a view to establishing whether the site or its contents are of interest) is unlikely to interfere with a person's reasonably held expectation of privacy and therefore is not likely to require a directed surveillance authorisation. But where a public authority is systematically collecting and recording information about a particular person or group, a directed surveillance authorisation should be considered. These considerations apply regardless of when the information was shared online. See also paragraph 3 6

3.6 Private information may include personal data, such as names, telephone numbers and address details. Where such information is acquired by means of covert surveillance of a person having a reasonable expectation of privacy, a directed surveillance authorisation is appropriate13

Example 1. A police officer undertakes a simple internet search on a name, address or telephone number to find out whether a subject of interest has an online presence. This 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. A customs officer makes an initial examination of an individual's online profile to establish whether they are of relevance to an investigation. This is unlikely to need an authorisation. However, if during that visit it is intended to extract and record information to establish a profile 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: A public authority undertakes general monitoring of the internet in circumstances where it is not part of a specific, ongoing investigation or operation to identify themes, trends, possible indicators of criminality or other factors that may influence operational strategies or deployments This activity does not require RIPA authorisation However, when this activity leads to the discovery of previously unknown subjects of interest, once it is decided to monitor those individuals as part of an ongoing operation or investigation, authorisation should be considered.

3 16 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 (taking account of the guidance at paragraph 3.6 above);

• 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

3 17 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 (see paragraph 4.32).

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.

Internet and Urgent Enquires

Example· An authorisation under the 2000 Act would not be appropriate where police officers conceal themselves to observe suspicious persons that they come across in the course of a routine patrol or monitor social media accounts during a public order incident.

General Observations

3.33 The general observation duties of many law enforcement officers and other public authorities do not require authorisation under the 2000 Act, whether covert or overt. Such general observation duties frequently form part of the legislative functions of public authorities, as opposed to the pre-planned surveillance of a specific person or group of people. General observation duties may include monitoring of publicly accessible areas of the internet in circumstances where it is not part of a specific investigation or operation.

Collateral Intrusion

4.14 In order to give proper consideration to collateral intrusion, an authorising officer or person considering issuing the warrant should be given full information regarding the potential scope of the anticipated surveillance or interference, including the likelihood that any equipment or software deployed may cause intrusion on persons or property other than the subject(s) of the application. If an automated system such as an online search engine is used to obtain the information, the authorising officer should be made aware of its potential extent and limitations. Material which is not necessary or proportionate to the aims of the operation or investigation should be discarded or securely retained separately where it may be required for future evidential purposes. The authorising officer or person considering issuing the warrant should ensure appropriate safeguards for the handling, retention or destruction of such material in accordance with chapter 9 of this code, as well as compliance with data protection requirements

4.15 Where it is proposed to conduct surveillance activity or property interference specifically against individuals who are not suspected of direct or culpable involvement in the overall matter being investigated, interference with the privacy or property of such individuals should not be considered as collateral intrusion but rather as intended intrusion Any such surveillance or property interference activity should be carefully considered against the necessity and proportionality criteria

4 16 Where a public authority intends to access a social media or other online account to which they have been given access with the consent of the owner, the authority will still need to consider whether the account(s) may contain information about others who have not given their consent. If there is a likelihood of obtaining private information about others, the need for a directed surveillance authorisation should be considered, particularly (though not exclusively) where it is intended to monitor the account going forward

Example: If an individual provides the police with passwords and log-in details for their personal social networking accounts in order to provide evidence of threats made against them, this would not normally require a directed surveillance authorisation If the police then decided to monitor the accounts for the purposes of obtaining further evidence of criminal activity by the author of the threats, they should consider applying for a directed surveillance authorisation in circumstances where private information is likely to be obtained. This is because the police would be acting with the intention to monitor an individual who has not consented to and may not be aware of the surveillance. The public authority will also need to consider the extent of the collateral intrusion into the privacy of others who may comment on or post information onto the accounts under surveillance.

Use of a Third Party

4 32 In some circumstances it may be appropriate or necessary for a public authority to work with third parties who are not themselves a public authority (such as an individual, company or non-governmental organisation) to assist with an investigation. Where that third party is acting in partnership with or under the direction of a public authority, then they are acting as an agent of that authority and any activities that third party conducts which meet the 2000 Act definitions of directed or intrusive surveillance or amount to property interference for the purposes of the 1994 or 1997 Act, should be considered for authorisation under those Acts by the public authority on whose behalf that activity is being undertaken. Similarly, a surveillance authorisation should also be considered where the public authority is aware that a third party (that is not a public authority) is independently conducting surveillance and the public authority intends to make use of any suitable material obtained by the third party for the purposes of a specific investigation being undertaken by that public authority

CHIS Codes Aug 18

Online Covert Activity

4 11 Any member of a public authority, or person acting on their behalf, who conducts activity on the internet in such a way that they may interact with others, whether by publicly open websites such as an online news and social networking

service, or more private exchanges such as e-messaging sites, in circumstances where the other parties could not reasonably be expected to know their true identity (as an official rather than private individual), should consider whether the activity requires a CHIS authorisation A directed surveillance authorisation should also be considered, unless the acquisition of that information is or will be covered by the terms of an applicable CHIS authorisation.

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

For example·

• An investigator using the internet to engage with a subject of interest at the start of an operation, in order to ascertain information or facilitate a meeting in person.

• Directing a member of the public (such as a CHIS) to use their own or another internet profile to establish or maintain a relationship with a subject of interest for a covert purpose.

• Joining chat rooms with a view to interacting with a criminal group in order to obtain information about their criminal activities.

4.13 A CHIS authorisation will not always be appropriate or necessary for online investigation or research. Some websites require a user to register providing personal identifiers (such as name and phone number) before access to the site will be permitted Where a member of a public authority sets up a false identity for this purpose, this does not in itself amount to establishing a relationship, and a CHIS authorisation would not immediately be required, though consideration should be given to the need for a directed surveillance authorisation if the conduct is likely to result in the acquisition of private information, and the other relevant criteria are met.

Example 1· An HMRC officer intends to make a one-off online test purchase of an item on an auction site, to investigate intelligence that the true value of the goods is not being declared for tax purposes. The officer concludes the purchase and does not correspond privately with the seller or leave feedback on the site No covert relationship is formed and a CHIS authorisation need not be sought.

Example 2· HMRC task a member of the public to purchase goods from a number of websites to obtain information about the identity of the seller, country of origin of the goods and banking arrangements The individual is required to engage with the seller as necessary to complete the purchases The deployment should be covered by a CHIS authorisation because of the intention to establish a relationship for covert purposes.

4 14 Where a website or social media account requires a minimal level of interaction, such as sending or receiving a friend request before access is permitted, this may not in itself amount to establishing a relationship Equally, the use of electronic gestures such as "like" or "follow" to react to information posted by others online would not in itself constitute forming a relationship However, it should be borne in mind that entering a website or responding on these terms may lead to further interaction with other users and a CHIS authorisation should be obtained if it is intended for an officer of a public authority or a CHIS to engage in such interaction to obtain, provide access to or disclose information

Example 1· An officer maintains a false persona, unconnected to law enforcement, on social media sites in order to facilitate future operational research or investigation. As part of the legend building activity he "follows" a variety of people and entities and "likes" occasional posts without engaging further. No relationship is formed and no CHIS authorisation is needed.

Example 2: The officer sends a request to join a closed group known to be administered by a subject of interest, connected to a specific investigation. A directed surveillance authorisation would be needed to cover the proposed covert monitoring of the site. Once accepted into the group it becomes apparent that further interaction is necessary. This should be authorised by means of a CHIS authorisation

4.15 When engaging in conduct as a CHIS, a member of a public authority should not adopt the identity of a person known, or likely to be known, to the subject of interest or users of the site without considering the need for authorisation. Full consideration should be given to the potential risks posed by that activity.

4.16 Where use of the internet is part of the tasking of a CHIS, the risk assessment carried out in accordance with section 6.13 of this code should include consideration of the risks arising from that online activity including factors such as the length of time spent online and the material to which the CHIS may be exposed. This should also take account of any disparity between the technical skills of the CHIS and those of the handler or authorising officer, and the extent to which this may impact on the effectiveness of oversight.

4.17 Where it is intended that more than one officer will share the same online persona, each officer should be clearly identifiable within the overarching authorisation for that operation, providing clear information about the conduct required of each officer and including risk assessments in relation to each officer involved. (See also paragraph 3.23)

5.29 Where an over-arching authorisation has been provided as a framework for investigators to establish an online presence intended to provide a basis for future enforcement activity, this should be treated as part of the same investigation or operation for renewal purposes. However, where this generic activity leads to a separate operation against subjects identified through the online presence, a fresh authorisation should be considered, and a decision taken on a case by case basis by reference to the factors listed in paragraph 5.28 above

OSC procedures & Guidance 2016

76. To assist an Authorising Officer to reach a proper judgment, the value of the data, information or intelligence on which the application has been made should be clear. It is considered best practice for law enforcement agencies to utilise standard evaluation nomenclature which grades both the source and the information. While it is not necessary or desirable in the application to spell out in detail the content of intelligence logs, cross-referencing to these enables an Authorising Officer to check detail. Particular care should be taken when using data or information obtained from open or unevaluated sources such as the Internet or social networks.

243. Covert Internet Investigators (now often referred to as undercover officers on line (UCOL)) may establish or maintain a relationship with more than one individual in relation to different investigations. If it is not possible to construct a single authorisation to cover all of the relationships (because the persons with whom relationships are established are not known in advance) it will be necessary to construct for each person with whom a relationship has been established a separate authorisation each of 12 months' duration. It is important that the same Authorising Officer considers each authorisation to ensure that operational conflict and risks do not develop and to monitor the security and welfare of the CHIS. When appropriate, reviews should be combined to establish whether separate authorisations can be combined into a single authorisation to reduce bureaucracy and error.

Covert Surveillance of Social Networking Sites (SNS)

289. The fact that digital investigation is routine or easy to conduct does not reduce the need for authorisation. Care must be taken to understand how the SNS being used works. Authorising Officers must not be tempted to assume that one service provider is the same as another or that the services provided by a single provider are the same.

289.1 Whilst it is the responsibility of an individual to set privacy settings to protect unsolicited access to private information, and 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 (instant messages for example) Where privacy settings are available but not applied the data may be considered open source and an authorisation is not usually required. Repeat viewing of "open source" sites may constitute directed surveillance on a case by case basis and this should be borne in mind.

289.2 Providing there is no warrant authorising interception in accordance with section 48(4) of the 2000 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)

289.3 It is not unlawful for a member of a public authority to set up a false identity but it is inadvisable for a member of a public authority to do so for a covert purpose without an authorisation for directed surveillance when private information is likely to be obtained The Senior Responsible Officer (SRO) should be satisfied that there is a process in place to ensure compliance with the legislation. Using photographs of other persons without their permission to support the false identity infringes other laws.

289 4 A member of a public authority should not adopt the identity of a person known, or likely to be known, to the subject of interest or users of the site without authorisation, and without the consent of the person whose identity is used, and without considering the protection of that person. The consent must be explicit (i.e. the person from whom consent is sought must agree (preferably in writing) what is and is not to be done).