Southwark Council
southwark.gov.uk

POLICY, PROCEDURES & FORMS
on
DIRECTED SURVEILLANCE
and use of
COVERT HUMAN INTELLIGENCE SOURCES
under the
REGULATION OF INVESTIGATORY POWERS ACT 2000
as amended by The Protection of Freedoms Act 2012

Version 13
Amended: August 2019

CONTENTS

NOTE:

This document must be read in conjunction with the Regulation of Investigatory Powers Act Codes of Practice issued by the Home Office on:

- Covert Surveillance & Property Interference 2018 ('CS CoP')
- Covert Human Intelligence Sources 2018 ('CHIS CoP')
- Acquisition Disclosure and retention of communications data 2015 ('Comms COP')
- Interception of communications 2016
- Equipment interference 2016
- Investigation of protected electronic information

And in respect of CCTV

- The Council's Code of Practice for CCTV Cameras ('CCTV CoP')
- The Surveillance Camera Commissioner's Surveillance camera Code of Practice 2014 ('SCC CoP')
- The Information Commissioner's code - In the Picture – A Data Protection Code of Practice for Surveillance Cameras and Personal Information.

This document must also be read in conjunction with the Procedures and Guidance issued by the Office of Surveillance Commissioners (December 2014).

Copies of this document, application forms, Codes of Practice and the Central Register of Trained Officers are located on *the Source* and are maintained by the corporate team in legal services. All queries should be referred to Norman Coombe and the governance team.

The Log of Authorisations, a password protected document, is visible to Authorising Officers only on *Legal Services Shared Drive R:RIPA/RIPA Log- Official*

SOUTHWARK COUNCIL POLICY & PROCEDURES
REGULATION OF INVESTIGATORY POWERS ACT 2000 (RIPA)

A Background

The Human Rights Act 1998 requires the council, and organisations working on its behalf, to have respect for the private and family life of citizens. However, in rare cases, it may be necessary for the council to act covertly in ways that could interfere with an individual's rights.

The Regulation of Investigatory Powers Act 2000 (RIPA) provides a mechanism for authorising directed surveillance and the use of a "covert human intelligence source" ('CHIS' - e.g. an informer or undercover agent). It aims to ensure that any interference with an individual's privacy is necessary and proportionate, and that both the public interest and the human rights of individuals are protected.

It also provides a mechanism for council staff to access limited information from telecommunications companies which are covered by separate, similar procedures.

It is important to note that the legislation does not just affect directly employed council staff. All external agencies working for Southwark Council automatically become a public body under the Act for the time they are working for the council. It is essential therefore that all external agencies comply with RIPA too, and that work carried out by agencies on the council's behalf be properly authorised by one of the council's designated Authorising Officers.

The Office of the Surveillance Commissioners (OSC) can inspect the council's policies and procedures and individual authorisations at any time. The OSC usually provide notice before an inspection, but can arrive unannounced. If the correct procedures are not followed the consequences can be serious. The evidence obtained may be ruled inadmissible. If officers are found to have acted in bad faith, a trial may be stopped as an abuse of process (*R v Sutherland* 2002 – police officers were found to have acted in bad faith in covertly recording conversations in the exercise yard between defendants and their solicitors). A complaint of maladministration might be made to the Ombudsman. The council could be made the subject of an adverse report to the Surveillance Commissioner. A claim could be made leading to the payment of compensation by the council. In any of these circumstances the council is likely to receive adverse publicity.

This document summarises the relevant provisions of RIPA, the Codes of Practice and government guidance. If in doubt as to the application of these provisions officers are asked to refer to the relevant Home Office Code/s of Practice (on The Source) and to contact the governance team in legal services (Norman Coombe – ext 57678) if in any doubt as to how to apply the provisions.

B Changes to the RIPA process

The Protection of Freedoms Act 2012 came into force on 1 November 2012 and requires all RIPA authorisations to obtain judicial approval by a court order before they can take effect.

The Regulation of Investigatory Powers (Directed Surveillance and Covert Human Intelligence Sources) (Amendment) Order 2012 also came into force on 1 November 2012 and limits the authorisation of directed surveillance to criminal offences which carry a custodial sentence of at least six months or relate to the sale of tobacco, alcohol and knives to children ("the directed surveillance crime threshold").

The 2018 Codes of Practice also reflect changes introduced by the Investigatory Powers Act 2016 (the 2016 Act) including the introduction of equipment interference warrants and the new oversight framework, establishing the Investigatory Powers Commissioner.

C What RIPA does and doesn't do - Surveillance

RIPA does

- require authorisation of directed surveillance.
- prohibit the council from carrying out intrusive surveillance.
- require authorisation of the conduct and use of a CHIS.
- require safeguards for the conduct and use of a CHIS.

RIPA does not

- make unlawful conduct which is otherwise lawful.
- prejudice any existing power to obtain information by any means not involving conduct that may be authorised under the Act. For example, it does not affect the council's current powers to obtain information via the DVLA or to obtain information from the Land Registry as to the owner of a property.
- apply to activities outside the scope of Part II of RIPA, which may nevertheless be governed by other legislation, including the Human Rights Act. A public authority will only engage RIPA when in performance of its 'core functions' – i.e. the functions specific to that authority as distinct from all public authorities [*C v The Police & Sec State for the Home Office 2006] [CS CoP 3.35].*

Legal advice should always be sought if there is any doubt as to whether the activity in question is a 'core function'.

D Types of Surveillance

"Surveillance" includes:

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

Surveillance can be overt or covert.

1 Overt Surveillance

Most of the surveillance carried out by the council will be done overtly – there will be nothing secretive, clandestine or hidden about it. In many cases, officers will be behaving in the same way as a normal member of the public (e.g. in the case of some test purchases), and/or will be going about council business openly (e.g. a market inspector walking through East Street market). Similarly, surveillance will be overt if the subject has been told it will happen (e.g. where a noisemaker is warned that noise will be recorded if the noise continues, or where an entertainment licence is issued subject to conditions and the licensee is told that officers may visit without identifying themselves to check that the conditions are being met.) The use of a tracking or recording device in a vehicle owned by the council is unlikely to be regarded as covert if the staff using the vehicle are notified that they are in place and their purpose.

2 Covert Surveillance

Surveillance is covert if, and only if, carried out in a manner calculated to ensure that persons subject to the surveillance are unaware it is or may be taking place (Section 26(9)(a) RIPA).

RIPA regulates two types of covert surveillance - Directed Surveillance and Intrusive Surveillance - and the use of Covert Human Intelligence Sources (CHIS).

3 Directed Surveillance

Directed Surveillance is surveillance which

- is covert surveillance; and
- is not intrusive surveillance (see definition below – the council must not carry out intrusive surveillance;
- is not carried out as an immediate response to events which would otherwise make seeking authorisation under the Act unreasonable e.g. spotting something suspicious and continuing to observe it; *[CS CoP 2.4, 3.1, 3.24]*;
- is not authorised as part of an equipment interference warrant under the 2016 Act;
- is undertaken for the purpose of a **specific investigation** or operation in a manner **likely to result in obtaining private information** about an individual (whether or not that person is specifically targeted for purposes of an investigation). *[Section 26(10) RIPA] [CS CoP 2.4, 3.1]*; and
- satisfies the directed surveillance crime threshold;
- can include online covert activity and aerial covert surveillance

4 Private information

Private information in relation to a person includes any information relating to his private or family life. The fact that covert surveillance occurs in a public place or on business premises does not mean that it cannot result in the obtaining of private information about a person. 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 [CS CoP 3.4]. Prolonged surveillance targeted on a single person may very well result in the obtaining of private information. Similarly, although overt town centre CCTV cameras do not normally require authorisation, if the camera is tasked for a specific operation, which involves prolonged surveillance on particular individual/s, authorisation may well be required *]*. The way in which a person runs her/his business may also reveal information about her or his private life . In deciding whether certain covert surveillance does, or does not, require a directed surveillance authorisation the potential applicant officer must carefully consider the issue of private information. In some circumstances the totality of information gleaned may constitute private information even if individual records do not. There are, for example, test purchase situations and covert inspection activities where it is unlikely that any private information will be obtained and therefore no authorisation is necessary. However in the event of subsequent legal proceedings such a decision could be subject to challenge. It is therefore recommended that a decision not to seek authorisation be made in consultation with an authorising officer and that the decision making process be documented in accordance with the relevant department's internal procedures.

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 section F below for further guidance about the use of the internet as a surveillance tool.

5 Directed surveillance crime threshold

- the council can only authorise use of directed surveillance under RIPA to prevent or detect criminal offences that are either punishable, whether on summary conviction or indictment, by a maximum term of at least 6 months' imprisonment.
- the council may also continue to authorise the use of directed surveillance for the purpose of preventing or detecting specified criminal offences under s146, 147 or 147A of the Licensing Act 2003 or s7 of the Children and Young Persons Act 1933 (relating to the underage sale of alcohol and tobacco) where the necessity and proportionality test is met and prior court approval has been granted.

Examples of cases where the offence being investigated attracts a maximum custodial sentence of six months or more could include more serious criminal damage, dangerous waste dumping and serious or serial benefit fraud. The council may not authorise the use of directed surveillance under RIPA to investigate disorder that does not involve criminal offences or to investigate low-level offences which may include, for example, littering, dog control and fly-posting *[CS CoP 4.44].*

6 Surveillance must be necessary and proportionate

RIPA provides that before granting an authorisation the Authorising Officer must be satisfied that the proposed surveillance is necessary for the prevention or detection of crime or the prevention of disorder and is proportionate to what is sought to be achieved by carrying it out. Surveillance will not be proportionate if the information sought could reasonably be obtained by less intrusive means. In particular, the Authorising Officer must consider both the gravity of the conduct under investigation and whether all reasonable alternative methods of obtaining the necessary outcome have been considered - and why they were discounted. *[CS CoP 4.4 – 4.10].*

Council Officers can carry out "Directed Surveillance" IF AND ONLY IF the RIPA authorisation procedures are followed.

7 Use of CCTV cameras

The use of temporary covert CCTV cameras at specified locations, e.g. flytipping 'hotspots', for the purpose of recording unlawful activities and obtaining photographic evidence of the suspect/s, carries with it not only the potential to obtain private information about the alleged offender/s but also the likelihood of collateral intrusion in to the activities of members of the public using the area under surveillance. In such circumstances authorisation will be required for directed surveillance.

Overt CCTV cameras which are permanently sited for the purposes of, for example, monitoring traffic flow or public safety will not generally require RIPA authorisation. Similarly, the overt use of ANPR systems to monitor traffic flow or detect motoring offences does not require an authorisation under RIPA. Members of the public should be made aware that such systems are in use e.g. clearly visible cameras or signage, through the provision of information and by undertaking consultation. The Protection of Freedoms Act 2012 places a statutory obligation on the council to have regard to the Surveillance Camera Code of Practice where surveillance is conducted overtly by means of a surveillance camera system in a public place. *[CS CoP 3.28].*

The council should also be aware of the relevant Information Commissioner's code ("In the Picture – A Data Protection Code of Practice for Surveillance Cameras and Personal Information").

However, there may be occasions when the council wishes to use such CCTV cameras for the purposes of a specific investigation or operation or to target a specific person. In such circumstances (unless as an immediate response to events) consideration must be given as to whether authorisation for directed surveillance is required *[CS CoP 3.31].* For example, authorisation for directed surveillance is likely to be required if the council wishes to make use of permanently sited overt CCTV cameras in circumstances where officers have received reports of unlawful trading and wish to use those existing CCTV systems to keep watch for such activities. However, authorisation would not be required where officers review existing CCTV footage of general filming in the area for evidence of past unlawful activity following such a report.

8 Collaborative working

If the council is acting on behalf of another agency, or vice versa, the tasking agency should normally obtain or provide the RIPA authorisation. Where the operational support of another agency (e.g. the Police) is foreseen, this should be specified in the authorisation *[CS CoP 4.30].*

For example, if the police wish to use the council's CCTV cameras for one of their investigations, this must be agreed by an Authorising Officer. A copy of the police RIPA authorisation form must be obtained and the details entered on the council's central register.

A council officer seeking an authorisation should be alert to any particular sensitivities in the local community and if necessary consult with a senior police officer to ensure that the proposed surveillance creates no conflict with the activities of other public authorities *[CS CoP 4.29].*

Where an individual or non-governmental organisation is acting under the direction of the council, they are acting as an agent of the council and any directed or intrusive surveillance they undertake must be considered for authorisation [CS CoP 4.32]. Similarly, a surveillance authorisation should also be considered where the council is aware that a non public authority third party is independently conducting surveillance and the council intends to make use of any suitable material obtained by that third party for the purposes of a specific investigation being undertaken by the council.

9 Intrusive Surveillance

- is covert
- relates to residential premises and private vehicles; and
- involves the presence of an individual on the premises or in the vehicle; or is carried out by a surveillance device. If a surveillance device is not on the premises or in the vehicle it is not intrusive, unless it consistently provides information of the same quality as if it was on the premises or in the vehicle
- also includes directed surveillance under the ambit of the Regulation of Investigatory Powers (Extension of Authorisation Provisions: Legal Consultations) Order 2010 [CS CoP 9.63-9.67].
- can be carried out <u>only</u> by police and other specified law enforcement agencies.

Council officers must not carry out intrusive surveillance.

10 Examples of different types of Surveillance

Surveillance will fall into one of four categories:

Type of Surveillance	Examples
Overt	• Police Officer or Parks Warden on patrol. • Signposted town centre CCTV cameras (in normal use) • Recording noise coming from premises after the occupier has been warned that this will occur if the noise persists. • Some test purchases (where the test purchaser behaves no differently from a normal member of the public).
Covert, but not requiring authorisation	• Hidden CCTV camera focused on a railway bridge which has just been cleared of graffiti, where it is expected that taggers will target the bridge. • Some test purchases (where the test purchaser behaves no differently from a normal member of the public).
Directed – requires RIPA authorisation.	• Officers follow an individual over the course of the day, to establish whether he is working when claiming benefit • Test purchases where the test purchaser has a concealed recording device which is likely to obtain private information about an individual (whether or not the shop keeper). • Installing surveillance equipment in a council owned vehicle to covertly monitor the occupants.
Intrusive - Council cannot do.	• Planting a listening device (bug) in a person's home or in their private motorcar.

Directed and Intrusive Surveillance are subject to the Covert Surveillance & Property Interference Code of Practice (CoP) issued under s 71 RIPA. The CoP is available on the Source.

E Conduct and Use of a Covert Human Intelligence Source (CHIS)

1 Who is a CHIS?

- A person is a CHIS if s/he establishes or maintains a personal or other relationship with a person for the covert purpose of obtaining information, or access to information, or covertly discloses information obtained by the use of such a relationship *[CHIS CoP 2.1]*.
- A covert purpose is one calculated to ensure that one of the parties to the relationship is unaware of the purpose.

- The Regulation of Investigatory Powers (Covert Human Intelligence Sources: Relevant Sources) Order 2013 further defines a "relevant source" as a CHIS who holds a position or office within a police force or the Home Office and enhanced authorisation arrangements are in place for this type of source (previously known as "undercover officers").

2 What must be authorised

The conduct or use of a CHIS requires authorisation.

- **Conduct** of a CHIS = establishing or maintaining a personal or other relationship with a person for the covert purpose of (or incidental to) obtaining and passing on information.
- **Use** of a CHIS = actions inducing, asking or assisting a person to act as a CHIS.

The Council can use a CHIS IF AND ONLY IF RIPA procedures are followed. Authorisation is advisable where the council intends to task someone to act as a CHIS.

3 European Convention on Human Rights (ECHR)

Authorisations for the use or conduct of a CHIS relate to the covert manipulation of a relationship to gain any information. ECHR case law makes it clear that Article 8 includes the right to establish and develop relationships. Accordingly, any manipulation of a relationship by a public authority is likely to engage Article 8, regardless of whether or not the public authority intends to acquire private information. The council should consider an authorisation whenever the use or conduct of a CHIS is likely to engage an individual's rights under Article 8, whether this is through obtaining information, particularly private information, or simply through the covert manipulation of a relationship. An authorisation will be required if a relationship exists between the subject and the CHIS, even if specific information has not been sought by the public authority. *[CHIS CoP 2.12-2.14]*

Legend Building - when a relevant source is deployed to establish their 'legend'/build up their cover profile, an authorisation must be considered under the 2000 Act if the activity will interfere with an individual's Article 8 rights. The individual does not have to be the subject of a future investigation. Interference with any individual's Article 8 rights requires authorisation under the 2000 Act. Where an authorisation is not considered necessary this should be decided by an Authorising Officer and arrangements should be in place to maintain active review of this position and *[CHIS CoP 2.16].*

4 Juvenile Source

Special safeguards apply to the use or conduct of juvenile sources (under 18). Only the Chief Executive can authorise the use of a juvenile source *[CHIS CoP 4.2]*. Under no circumstances can a child under 16 years of age be authorised to give information against his or her parents or any person who has parental responsibility. The duration of an authorisation is one month.

5 Vulnerable individuals

A vulnerable individual is a person who by reason of mental disorder or vulnerability or other disability, age or illness is or may be unable to take care of themselves, or unable to protect themselves against significant harm or exploitation. A vulnerable individual should only be authorised to act as a CHIS in the most exceptional circumstances. Only the Chief Executive can authorise the use of a vulnerable person as a CHIS *[CHIS CoP 4.1].*

6 Test Purchases

If a source is to be asked to obtain information, provide access to information or otherwise to act for the benefit of the council, then a CHIS authorisation for the use or conduct of that source will be required in advance of any such assignment which requires the source to establish or maintain a 'personal or other relationship' for a covert purpose. In this context 'establish' simply means 'set up' (as distinct from 'maintain'), so that even a single transaction –e.g. in the case of a test purchase – *may* constitute a relationship. Repetition is not always necessary to give rise to a relationship, but whether or not a relationship exists depends on all the circumstances including the length of time of the contact between the seller and buyer and the nature of any covert activity *[CHIS CoP 2.15]*. Some assignments are unlikely to require the source to establish a personal or other relationship for a covert purpose – e.g. if the source's assignment is limited to gathering factual information about the layout of commercial premises.

If a council officer, or another person acting under the instructions of a council officer, enters a shop in the normal course of business and purchases a product available for sale over the counter then a CHIS authorisation will not normally be required. However, unless the test purchaser is to be instructed not to enter in to *any* conversation with the shopkeeper then consideration must be given as to whether there is the possibility of a 'relationship' which would require a CHIS authorisation.

If an officer develops a relationship with a shopkeeper in order to obtain information about the source of the allegedly illegal products on sale, then the officer will require a CHIS authorisation.

If a council officer, or another person acting under the instructions of an officer, uses any covert recording device (camera and/or audio) to record events in the shop then an authorisation will be required for directed surveillance *[CS CoP 2.2 & CHIS CoP 3.25-3.27]*.

A combined authorisation can be granted when a CHIS is also carrying out directed surveillance *[CS CoP 4.17 & CHIS CoP 3.20-3.22.*

7 Members of the Public

The provisions of RIPA are not intended to apply in circumstances where members of the public volunteer information to the council as part of their normal civic duties, or to contact numbers set up to receive information. Members of the public who volunteer information to the council, whether anonymously – e.g. by means of a telephone line set up for that purpose – or otherwise, will not normally be considered to be a CHIS. However, if a member of the public is asked to e.g. watch out for and diarise particular activities at specific times about another person with whom they have a relationship (whether personal or not) then this would amount to directed surveillance and a CHIS authorisation would be required *[CHIS CoP 2.18]*. An authorisation should also be considered where the council becomes aware that a third party is independently maintaining a relationship ("self-tasking") in order to obtain evidence of criminal activity, and the council intends to make use of that material for our own investigative purposes *[CHIS CoP 2.26].*

8 Noise

Persons who complain about excessive noise, and are asked to keep a noise diary, will not normally be a CHIS, as they are not required to establish or maintain a relationship for a covert purpose. Recording the level of noise (e.g. the decibel level) will not normally capture private information and therefore does not require authorisation. Recording sound with a DAT recorder on private premises could constitute intrusive surveillance unless it is done overtly – for example it will be possible to record sound if the noisemaker is warned that this will occur if the level of noise continues.

F ONLINE COVERT ACTIVITY

1 Background

The use of the internet may be required to gather information prior to and/or during an operation, which may amount to directed surveillance. Alternatively an investigator may need to communicate covertly online, for example, contacting individuals using social media websites which may require a CHIS authorisation.

Whenever the council intends to use the internet as part of an investigation, we must first consider whether the proposed activity is likely to interfere with a person's Article 8 rights, including the effect of any collateral intrusion. Any activity likely to interfere with an individual's Article 8 rights should only be used when necessary and proportionate to meet the objectives of a specific case.

2 Directed Surveillance [CS CoP 3.10-3.16]

A preliminary examination with a view to establishing whether a site or its contents are of interest is unlikely to interfere with a person's reasonably held expectation of privacy but where information about a particular person or group is systematically collected and recorded a directed surveillance authorisation should be considered, regardless of when the information was shared online (CS CoP 3.15).

Where it is considered that private information is likely to be obtained, an authorisation (combined or separate) must be sought.

In order to determine whether a directed surveillance authorisation should be sought 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 include whether:

- The investigation or research is directed towards an individual or organisation;
- It is likely to result in obtaining private information about a person or group;
- It is likely to involve visiting internet sites to build up an intelligence picture or profile;
- The information obtained will be recorded and retained;
- The information is likely to provide an observer with a pattern of lifestyle;
- The information is being combined with other sources of information or intelligence, which amounts to information relating to a person's private life;
- The investigation or research is part of an ongoing piece of work involving repeated viewing of the subject
- 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.

Where the council intends to access an online account to which they have been given access with the consent of the owner, the council will still need to consider whether the account may contain information about others who have not given their consent and whether an authorisation is still required.

3 Conduct or Use of a CHIS [CHIS CoP 4.10 – 4.16]

Any council officer, or person acting on our behalf, who conducts activity on the internet in such a way that they may interact with others, whether by publicly open websites or more

private exchanges, in circumstances where the other parties could not reasonably be expected to know their true identity, should consider whether the activity requires a CHIS authorisation.
Factors that should be considered include:

- Is a council officer or member of the public being tasked by the council to use an internet profile to establish or maintain a relationship with a subject of interest for a covert purpose (authorisation is likely to be required);
- Setting up a false identity online does not in itself amount to establishing a relationship;
- A minimal level of interaction e.g. friend requests, likes, follows, may not in itself amount to establishing a relationship
- Further interaction with other users, engagement in such interactions to obtain, provide access to or disclose information would require a CHIS authorisation;
- Adopting the identity of a person known to a subject of interest requires consideration of the need for an authorisation and of the potential risks;

4 Social Media and online covert activity policy

Use of social media for the gathering of evidence to assist in enforcement activities must also comply with the policy set out below:

- It is not unlawful for a council officer to set up a false identity but it is inadvisable to do so for a covert purpose without authorisation. Using photographs of other persons without their permission to support the false identity infringes other laws.
- Where it is necessary and proportionate for officers pursuing an investigation to create a false identity in order to 'friend' individuals on social networks a CHIS authorisation must be obtained. If such activity is likely to result in the obtaining of private information, a Directed Surveillance authorisation (combined with a CHIS authorisation or separate) must be obtained.
- Authorisation for the use and conduct of a CHIS is necessary if a relationship is established or maintained by a council officer (i.e. the activity is more than mere reading of the site's content). Where activity is only carrying out a test purchase a CHIS authorisation may not be necessary but this should be confirmed with the Authorising Officer on a case by case basis.
- Where privacy settings are available but not applied, the data may be considered open source and an authorisation is not usually required.
- Officers viewing an individual's open profile on a social network should do so as infrequently as possible in order to substantiate or refute an allegation
- Where repeated viewing of open profiles on social networks is necessary and proportionate to gather further evidence or to monitor an individual's status, then RIPA authorisation must be considered as repeat viewing of "open source" sites may constitute directed surveillance on a case by case basis.. Any decision not to seek authorisation be made in consultation with an authorising officer and that the decision making process be documented in accordance with the relevant department's internal procedures.
- Officers should be aware that it may not be possible to verify the accuracy of information on social networks and, if such information is to be used as evidence, take reasonable steps to ensure its validity.

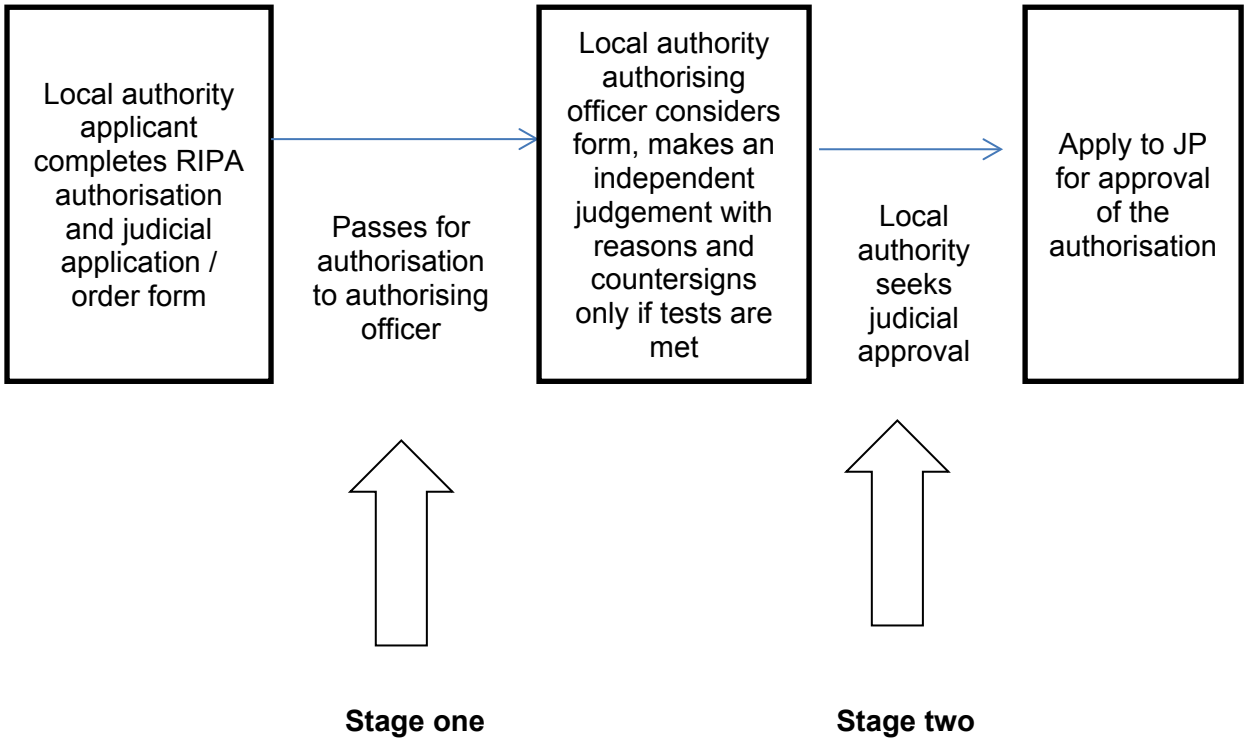
Consideration should always be given to RIPA implications when accessing social media and personal sites for surveillance purposes.

G Applications for Authorisation and Approval

Directed surveillance and the use of a CHIS can only be carried out if the proper two stage RIPA authorisation and approval process is followed:

- Stage one - internal authorisation
- Stage two - approval by a Magistrate.

DIRECTED SURVEILLANCE/CHIS (COVERT HUMAN INTELLIGENCE SOURCE)



Appendix 1 provides a flow chart of process from application consideration to recording of information.

H Stage One – Internal Authorisation

1 Application Forms

Applications for authorisation should be made in writing using standard RIPA forms. The forms are designed to ensure that the criteria for RIPA are fully considered.

Southwark uses modified Home Office forms included in Appendix 3 and also available on The Source. Forms were amended in November 2012 – previous versions should not be used.

The Application Form must now be accompanied by the partly completed Magistrates Court Application Form.

2 Grounds for Authorisation

Directed Surveillance, or the Conduct and Use of a CHIS can be authorised by the council only:

- **For the prevention or detection of crime or the prevention of disorder**

Since January 2004 the council **can not** authorise surveillance on the following grounds:

- 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 the government.

The council has never been able to authorise surveillance on either of the following grounds which are restricted to some central government organisations:

- National Security
- Economic Interests of the UK

[See also Sections 28 & 29 RIPA, *CS CoP 5.1* & *CHIS CoP 5.1*]

3 Guidance for Applicants – Directed Surveillance

When completing an application for an authorisation the council 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 of information which weakens the case for the authorisation *[CS CoP 4.10]*.

The information provided on the application form should:

- identify the nature of the surveillance and the means by which it is to be undertaken;
- specify when the surveillance is to start and the length of time it is expected to continue;
- explain why the applicant believes that the proposed surveillance is necessary for the prevention or detection of crime or the prevention of disorder (as appropriate);
- identify what is sought to be achieved by the proposed surveillance;
- identify the offence which satisfies the directed surveillance crime threshold
- explain why the applicant considers the proposed surveillance is proportionate, having regard to the gravity and extent of the activity under investigation;
- explain why the proposed surveillance is a reasonable method of obtaining the necessary outcome;
- include the identities, where known, of those to be the subject of the surveillance;
- provide a summary of the intelligence case;
- the details of any confidential or privileged information that is likely to be obtained as a consequence of the surveillance;
- an assessment of the exception and compelling circumstances where information is subject to legal privilege;
- identify whether other reasonable means of obtaining information have been considered and why they have been discounted;
- explain how and why the proposed surveillance will cause the least possible intrusion on the intended subject/s;
- include an assessment of the risk of any collateral intrusion and details of any measures taken to limit this and why any intrusion is justified *[CS CoP 4.11 – 4.16]*;
- avoid any repetition of information

4 Guidance for Applicants – Conduct and Use of a CHIS

When completing an application for an authorisation the council 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 of information which weakens the case for the authorisation *[CHIS CoP 5.14]*.

The information provided on the application form should:

- identify the purpose for which the CHIS will be tasked or deployed (e.g. counterfeit sales);
- identify the nature of the conduct and use of the CHIS and the period of time it is expected to continue;
- explain why the applicant believes that the proposed conduct and use is necessary for the prevention or detection of crime or the prevention of disorder (as appropriate);
- explain how each activity to be authorised is expected to bring a benefit to the investigation;
- explain how and why the proposed conduct and use is proportionate to the intelligence dividend it hopes to achieve, having regard to the gravity and extent of the activity under investigation;
- explain how and why the methods to be adopted will cause the least possible intrusion to the subject/s;
- include an assessment of the risk of any collateral intrusion and details of any measures taken to limit this;
- detail any material subject to legal privilege or other confidential material that may be obtained as a consequence of the authorisation;
- where the intention is to acquire knowledge of matters subject to legal privilege, the exceptional and compelling circumstances that make the authorisation necessary;
- identify whether other reasonable methods of obtaining information have been considered and why they have been discounted;
- ensure the confidentiality of the CHIS – i.e. not include information which could lead to the identification of the CHIS;
- avoid any repetition of information.

Surveillance will not be proportionate if the information which is sought could reasonably be obtained by other less intrusive means.

5 Guidance for Authorising Officers

Authorisations can only be granted by the Authorising Officers listed in **Appendix 2.**

Authorisation under RIPA is quite separate from delegated authority to act under the council's scheme of delegation and internal departmental schemes of management. RIPA authorisations are for specific investigations only, and must be cancelled or renewed once the specific surveillance is complete or about to expire.

The Authorising Officer should not just "sign off" an authorisation, but must give **personal consideration** to the necessity and proportionality of the proposed action and must personally ensure that the surveillance is reviewed and cancelled within the applicable timescales.

6 Assessing the Application Form

When considering whether to authorise surveillance an Authorising Officer must:

- Consider the relevant Code/s of Practice;

- Satisfy him/herself that the authorisation is **necessary** in the circumstances of the particular case to prevent or detect crime *[CS CoP 4.4-4.10 & CHIS CoP 3.2-3.6]* and that the specified offence satisfies the directed surveillance crime threshold *[CS CoP 4.4410]*;

- Satisfy him/herself that the surveillance is **proportionate** to what it seeks to achieve *[CS CoP4.4-4.10 & CHIS CoP 3.2-3.6]*. In assessing whether or not the proposed surveillance is proportionate, the Authorising Officer will consider other appropriate means of gathering information and the degree of intrusiveness of the actions tasked on or undertaken by the CHIS;

  If there is an alternative practicable means of carrying out the surveillance, which is less intrusive, then the surveillance is neither necessary nor proportionate and should not be authorised.

- Take into account the risk of intrusion into the privacy of persons other than the specified subject of the surveillance (**Collateral Intrusion**). Measures must be taken wherever practicable to avoid collateral intrusion *[CS CoP 4.11-4.16 & CHIS CoP 3.5, 3.9-3.12];*

- Set a date for review of the authorisation; this should not exceed one month from the date of the grant of the authorisation *[CS CoP 4.34-4.39 & CHIS CoP 3.13-3.17]*;

- Record the expiry date of the authorisation on the application form. This will be three months (Directed Surveillance) or twelve months/one month (CHIS/juvenile CHIS) less one day from the date of the grant of the authorisation.

- Allocate a Universal Reference Number (URN) for the application. The URN will consist of two letters plus a number (see section I – Records Maintenance); and

- Ensure that the departmental log is completed, and that a copy of the entry in the log is forwarded to the Monitoring Officer's Central Log (Norman Coombe – ext 57678).

7 Additional Factors when Authorising a CHIS

In addition, when authorising the conduct or use of a CHIS the Authorising Officer must:

- be satisfied that the **conduct** and/or **use** of the CHIS is proportionate to what is sought to be achieved;

- be satisfied that appropriate arrangements are in place for the **management and oversight** of the CHIS, in particular the appointment of a named 'handler' to direct and record the day to day activities of the CHIS and monitor the CHIS's security and welfare; and the appointment of a named 'controller' to be responsible for the management of the handler and general oversight of the use of the CHIS *[CHIS CoP 6.5-6.9];*

- consider the likely degree of intrusion of all those potentially affected;

- ensure that a risk assessment is carried out to determine the risk to the CHIS of the activities to be undertaken and the likely consequences should the CHIS's role become known*[CHIS CoP 6.13-6.15];*

- consider any adverse impact on community confidence that may result from the use or conduct or the information obtained; and

- ensure **records** contain statutory particulars and are not available except on a 'need to know' basis.

  [See also *CHIS CoP Chapter 5 & 6*]

8 Duration of Authorisations

- The authorisation **must be cancelled** once it is no longer needed, and otherwise lasts for a maximum of 3 months for Directed Surveillance and 12 months for a CHIS (one month for a juvenile). Even in instances where it is anticipated that an authorisation will only be required for a period of time less than three months, authorisation should still be granted for the statutory three month period, subject to review at an interval reflecting expected duration, and the authorisation cancelled when it is no longer necessary *[CS CoP 5.14].*

9 Review and Cancellation

Review: The Authorising Officer must review authorisations at regular recorded intervals (normally not more than one month) and must cancel an authorisation if s/he becomes satisfied that the surveillance or use of a CHIS is no longer required or appropriate. The review of the use of a CHIS should include the use made of the CHIS during the period authorised; the tasks given to the CHIS; the information obtained from the CHIS; and the reasons why executive action is not possible at this stage. The results of a review should be retained for at least three years. Frequent reviews should occur where the use of a CHIS provides access to confidential information or involves significant collateral intrusion. *[CHIS CoP 5.19, 8.9-8.11*

The authorising officer should determine how often a review should take place. This should be as frequently as is considered necessary and practicable, but should not prevent reviews being conducted in response to changing circumstances.

During a review, the reviewing officer may amend aspects of the authorisation, for example to cease directed surveillance against one of a number of named subjects or to discontinue the use of a particular tactic.

Cancellation: The authorising officer who granted or renewed the authorisation must cancel it if they are satisfied that the use of the surveillance or the use or conduct of the CHIS longer satisfies the criteria for authorisation or that arrangements for the CHIS's case no longer satisfy the requirements described in section 29 of the 2000 Act. Where necessary, the safety and welfare of the CHIS should continue to be taken into account after the authorisation has been cancelled. The Authorising Officer will wish to satisfy themselves that all welfare matters are addressed *[CHIS CoP 5.31 & 5.32].* When cancelling the authorisation the Authorising Officer should record whether the surveillance was effective, necessary and met its objectives. Cancellations must be made using the cancellation form . If during an investigation it becomes clear that the activity being investigated does not amount to an offence which would meet the directed surveillance crime threshold, or the authorisation is no longer necessary or proportionate, the Applicant

must submit an application to an Authorising Officer for the authorisation to be cancelled. Cancellations do not need to be submitted for court approval.*[CS CoP 5.22 – 5.24].*

If it becomes necessary to amend the terms of an authorisation to reflect information gathered in the course of surveillance then a review should be conducted for that purpose. For example, if a directed surveillance authorisation provides for the surveillance of unidentified individuals whose identity is later established, the terms of the authorisation should be refined at a specially convened review to include the identity of these individuals *[CS CoP 4.39 & CHIS CoP 3.15 – 3.17].*

10 Renewals

Authorisations can be renewed in writing prior to expiry of the maximum period. The Authorising Officer must consider the matter afresh by carrying out a further review, including taking into account the information obtained and benefits of the surveillance to date, why it is considered necessary for the authorisation to continue and any collateral intrusion that has occurred *[CS CoP 5.16 – 5.21 & CHIS CoP 5.20-5.30].*

The renewal will begin on the day when the authorisation would have expired. Authorisations may be renewed more than once if still considered necessary and proportionate. **All renewals must also now be approved by the court.**

11 Urgent Authorisations

Urgent oral authorisations can no longer be granted. ALL authorisations must be in writing and submitted to the court with the completed court form. In exceptional circumstances an out of hours court application may be made but a signed written authorisation will still need to be produced to the court (see below).

I Stage two – Approval by a magistrate *[CS CoP 4.42 & CHIS CoP 3.28]*

1 Arrange a hearing

The first stage of the process is for the council to contact Her Majesty's Courts and Tribunals Service (HMCTS) administration team at the magistrates' court to arrange a hearing.

2 Documents

The court will need:-

- Sight of the original signed authorisation (plus a copy) and any supporting documents
- A partially completed judicial application order form (see Appendix 3) counter-signed by an Authorising Officer

These documents MUST by themselves make the case. It is not sufficient for the council to provide oral evidence where this is not reflected or supported in the papers provided. The magistrate may note on the form any additional information he or she has received during the course of the hearing but information fundamental to the case must be included in the authorisation form.

In order to maintain privacy, notice of the application is not required to the person whom the authorisation concerns or that person's legal representatives.

3 Attending a Hearing

The hearing is a 'legal proceeding' and therefore local authority officers need to be formally designated to appear, be sworn in and present evidence or provide information as required by the Magistrate.

The hearing will be in private (not in open court) and no press, public, the subject of the investigation or the subject's legal representative will be present. The application will be heard by a single Magistrate who will read and consider the RIPA authorisation or notice and the judicial application/order form. S/he may have questions to clarify points or require additional reassurance on particular matters and therefore the case investigator should attend as they will know the most about the investigation and will have determined that use of a covert technique is required in order to progress a particular case.

The council's constitution designates chief officers as being able to authorise certain officers for the purpose of presenting RIPA cases to the court under section 223 of the Local Government Act 1972. Chief officers should give such authorisations in writing and make a record of who is authorised.

Where such officers are authorised an officer from legal services is not required to attend the hearing. The Authorised Officer is also not required to attend the hearing but should, if possible, be contactable by phone to assist and advise the officer attending the hearing as and when required.

4 Decision

The magistrate 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;
- there continues to be reasonable grounds;
- the person who granted the authorisation was an appropriate designated person within the local authority
- the authorisation was made in accordance with any applicable legal restrictions, for example that the crime threshold for directed surveillance has been met.

The Magistrate may decide to:-

- **Approve the grant or renewal of an authorisation** - The grant or renewal of the RIPA authorisation will then take effect and the council may proceed to use the technique in that particular case.

- **Refuse to approve the grant or renewal of an authorisation or notice** - The RIPA authorisation will not take effect and the local authority may not use the technique in that case. A technical error in the form may be remedied without going through the internal authorisation process again and the council can then reapply for judicial approval once those steps have been taken. If more information is required to determine whether the authorisation or notice has met the tests then

the Magistrate will refuse the authorisation and the internal authorisation will need to be amended and re-authorised before being re-submitted to the court.

- **Refuse to approve the grant or renewal and quash the authorisation or notice** This applies where a magistrates' court refuses to approve the grant, giving or renewal of an authorisation or notice and decides to quash the original authorisation or notice. The court must not exercise its power to quash that authorisation or notice unless the applicant has had at least 2 business days from the date of the refusal in which to make representations.

5 Emergency Applications

On the rare occasions where out of hours access to a Magistrate is required the council has made the following arrangements:

- Two partially completed judicial application/order forms must be provided so that one can be retained by the Magistrate. The council should provide the court with a copy of the signed judicial application/order form the next working day.

However, in most emergency situations where the police have power to act, then they are able to authorise activity under RIPA without prior Magistrate's approval. No RIPA authority is required in immediate response to events or situations where it is not reasonably practicable to obtain it (for instance when criminal activity is observed during routine duties and officers conceal themselves to observe what is happening).

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

J Record maintenance and Safeguards

The Council must keep a secure centrally retrievable record of all authorisations, reviews, renewals, and cancellations *[CS COP 8.1-8.2 & CHIS CoP 7.1-7.3]*

1 Universal Reference Number for Authorisations

The Authorising Officer must allocate a Universal Reference Number (URN) to each application, consisting of initials identifying the department and a sequential number identifying the application number:

URN	Department
CE 001-	Chief Executives
CAS 001-	Children's and Adults' Services
EL 001-	Environment and Leisure
HCS 001-	Housing andModernisation
FCS 001-	Finance and Governance
PAB 001 -	Place and wellbeing

2 Records maintained in the Department

The following documents must be retained in the department:

- a copy of the application and a copy of the authorisation together with any supplementary documentation and notification of the authorisation given by the Authorising Officer;
-
- a record of the period over which the surveillance has taken place;
- the frequency of reviews prescribed by the Authorising Officer;
- a record of the result of each review of the authorisation;
- a copy of any renewal of an authorisation, together with the supporting documentation submitted when the renewal was requested;
- a copy of the court application and the order approving or otherwise the grant or renewal of any authorisation from a Justice of the Peace;
- the date and time when any instruction to cease surveillance was given;
- the date and time when any other instruction was given by the Authorising Officer.
- The Universal Reference Number for the authorisation (URN)

The applicant and Authorising Officer should retain a secure electronic copy of all documents generated. The Authorising Officer should update the secure electronic central register (log) to reflect the documents generated. The Authorising Officer should then promptly forward all original documents generated - authorisations, reviews, renewals, cancellations, court applications and orders - to the Monitoring Officer's nominee, who is responsible for maintaining the central register of all directed surveillance and CHIS operations undertaken.

The same principles of record keeping apply to applications which are refused .

A separate record should be maintained for human sources who do not meet the definition of a CHIS – e.g. members of the public who volunteer information on a repeated basis – as this will assist Officers in determining if and when that source may become a CHIS. This should be updated regularly to explain why authorisation is not considered necessary **Such decisions should be made by an Authorising Officer.** *[CHIS CoP 7.5].*

Copies of authorisations, reviews, renewals and cancellations may be disclosed in legal proceedings. If proper records are not maintained, evidence gathered may be inadmissible.

3 Records maintained centrally by the Monitoring Officer

Authorising Officers must forward the original of each authorisation, review, renewal, cancellation form, court application form and court order to the Monitoring Officer's nominee - currently Norman Coombe (Legal Services – ext 57678). On receipt, the Monitoring Officer's nominee will check that the electronic log accurately reflects the contents of these documents and thereafter secure them in a locked cabinet for use in the maintenance of the council's central register.

An electronic log is maintained centrally on restricted public folders. The Log is kept in a password-protected excel spreadsheet, located on the Legal Services Shared Drive R:RIPA/RIPA Log - official. The document is password protected, and the folder is

restricted so that only Authorising Officers and the Monitoring Officer's nominee can access it.

The Council must retain surveillance records for a period of at least three years from the ending of the authorisation *[CS CoP 8.1]* and it is desirable if possible to retain records for up to five years [CS CoP 8.5]. CHIS authorisation records should be retained for at least five years from the ending of the authorisation *[CHIS CoP 7.1].* The council must ensure the secure destruction of material no longer required *[CS CoP 9.22 & CHIS CoP 8.21].*

4 Safeguards

Officers must ensure that their actions when handling information obtained by means of covert surveillance or the use of CHIS comply with the relevant legal framework and the Code of Practice so 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, including data protection requirements, will ensure that the handling of private information is lawful, justified and strictly controlled and is subject to robust and effective safeguards. *[CS CoP Chaper 9 & CHIS CoP Chapter 8]*.

All material obtained under a surveillance authorisation or through the use or conduct of a CHIS must be handled in accordance with [safeguards which the council has implemented in line with the requirements of the Codes of Practice].

K Oversight, Errors, Review and Amendments

1 Oversight Procedures (internal)

The Senior Responsible Officer (SRO) shall establish and maintain regular meetings not less than twice a year with the Authorising Officers to check and test processes, review errors and address any training requirements. The SRO shall arrange an oversight meeting as soon as practicable following an inspection to discuss issues and outcomes as appropriate and will produce a written record of each review.

The SRO shall record any issues arising out of authorisation applications, the statutory considerations, reviews and cancellations and shall review the quality of authorisations granted from time to time.

The SRO shall carry out analysis of such issues and shall decide appropriate feedback to the Authorising Officers. Such information and conclusions shall also be reported to Standards Committee.

The SRO should be a member of the corporate leadership team and should be responsible for ensuring that all authorising officers are of an appropriate standard *[CS CoP 3.34].*

2 Oversight (external)

The Investigatory Powers Act provides for an Investigatory Powers Commissioner whose remit includes providing comprehensive oversight of the use of the powers in the Codes of Practice. Anyone, including any officer of the council, who has concerns about the way that investigatory powers are being used may report their concerns to the Commissioner *[CS CoP Chapter 10 & CHIS CoP Chapter 9].*

The Investigatory Powers Tribunal (IPT) has jurisdiction to investigate and determine complaints against the council's use of investigatory powers made by an individual or an organisation.*[CS CoP Chapter 11 & CHIS CoP Chapter 10].*

3 Errors

Any error, for example surveillance taking place without authority, failure to comply with the process set out in this guide, must be immediately notified to the SRO who will log the details and commence an initial review. Where this initial review determines that the error is a "relevant error" *[CS CoP 8.8]* or where the Council relied on information now found to be incorrect *[CS CoP 8.14]* this will be notified by the SRO to the Investigatory Powers Commissioner as soon as reasonably practicable and no later than ten working days after it has been established that a relevant error has occurred. The SRO will then undertake a comprehensive review and send a full report to the Investigatory Powers Commissioner as soon as reasonably practicable including information on the cause of the error; the amount of surveillance 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.

The Investigatory Powers Commissioner will inform a person of a relevant error relating to that person if they consider the error to be a serious error and it is in the public interest for the person concerned to be informed of the error. The Commissioner will ask the council for submissions and the council must take all steps required by the Commissioner to help identify the subject.

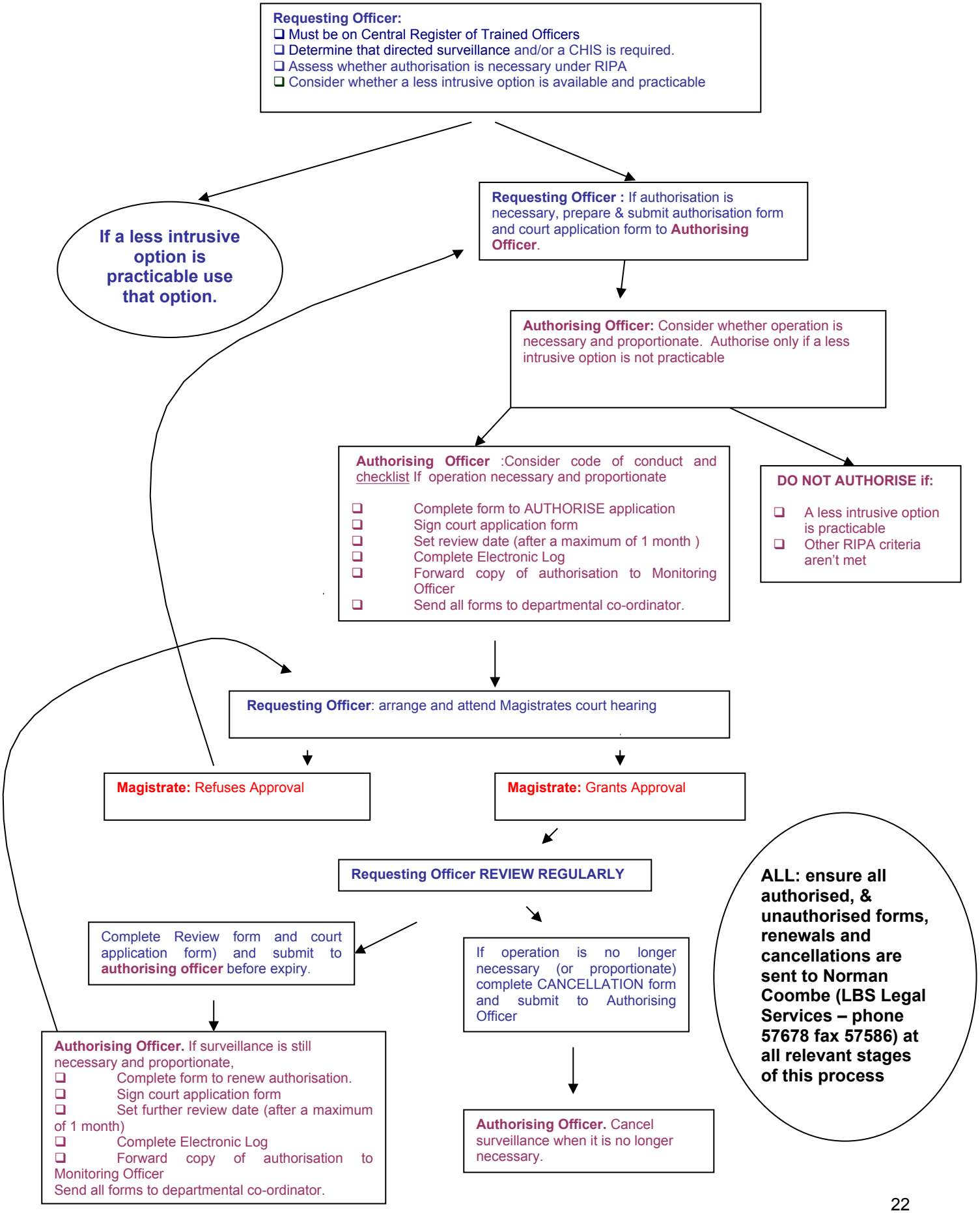
4 Review

The members of the Audit, Governance and Standards Committee shall review the use of RIPA 2000 and this policy at least once a year and the policy will also be reviewed every two years and approved by the relevant Cabinet Member. In order to facilitate this, the SRO shall provide regular reports to Audit, Governance and Standards Committee meetings on how RIPA 2000 has been used and whether there are any concerns as to the policy.

5 Amendments To This Policy And Procedures

The Monitoring Officer is duly authorised to keep this guidance document up to date, and to amend, delete, add or substitute any provisions as s/he deems necessary. For administrative and operational effectiveness, s/he is also authorised to amend the list of Authorising Officers set out in Appendix 2, by adding, deleting or substituting any posts.

Appendix 1 Flow chart of process



Up to date copies are available on *The Source*

Appendix 2 Authorising Officers

Authorising Officers must be a Director, Head of Service, Service Manager or equivalent *[RIPA Order 2010 Schedule 1 Part 1*]. The Authorising Officer should not be directly involved in the investigation. Authorising Officers are listed below.

The Chief Executive

ONLY the Chief Executive, Eleanor Kelly (or in her absence the person acting as CEO) can authorise:

- the use of a juvenile (i.e. under 18) or a Vulnerable Person to be a CHIS *[CHIS CoP Annex A]*
- Operations where knowledge of privileged or confidential information is likely to be acquired. This includes confidential personal information, confidential constituent information, confidential journalistic material and communications subject to legal privilege. Confidential personal information includes information held in confidence relating to the physical or mental health or spiritual counselling of a person who can be identified from it. *[CS CoP 12 Annex A & CHIS CoP 8.26-8.36 Annex A].*

Legal advice should always be sought in these circumstances.

Other Authorising Officers

The council's Authorising Officers can authorise applications from any department but should be independent of the investigation in respect of which authorisation is sought. In the event that no independent Authorising Officer can be contacted, application forms should be sent to the Monitoring Officer's nominee - currently Norman Coombe (ext 57678).

With effect from 2 July 2017 the Authorising Officers are:

Doreen Forrester-Brown, Director of Law and Democracy (phone 57502, fax 57586)

Dominic Cain, Director of Exchequer (phone 50636)

Stephen Gaskell, Head of Chief Executive's Office (phone 57293)

David Littleton, Head of Regulatory Services (phone 55725)

Senior Responsible Officer

The Senior Responsible Officer (SRO) is responsible for ensuring the integrity of the Council's processes for authorising directed surveillance and the use of CHIS's and ensuring compliance with RIPA and is the principal point of contact with the Office of Surveillance Commissioners and Inspectors when they conduct their inspections. The Council's Senior Responsible Officer is Doreen Forrester-Brown, Director of Law and Democracy and the Council's Monitoring Officer.

Appendix 3 Forms

Authorisation - Directed Surveillance

- Application
- Cancellation
- Review
- Renewal

Authorisation - CHIS

- Application
- Cancellation
- Review
- Renewal

Court Approval Application/Order

ANNEX A

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