SLOUGH BOROUGH COUNCIL

REGULATION OF INVESTIGATORY POWERS ACT 2000

(RIPA)

COVERT SURVEILLANCE POLICY AND PROCEDURAL GUIDANCE

July 2013
[Version 65 update – ~~February 2020~~June 2023]

CONTENTS

Note
This Policy has been revised as a result of The Investigatory Powers Act 2016
CS / COP = Covert Surveillance Code of Practice (August 2018)
CHIS / COP = CHIS Code of Practice (December 2022~~August 2018~~)

1. Introduction to RIPA

1.1 RIPA is an acronym for the Regulation of Investigatory Powers Act 2000. RIPA was introduced to ensure that Surveillance and certain other intelligence gathering complies with the European Convention of Human Rights and Fundamental Freedoms (ECHR), importantly Article 8 which provides:-

> *i) Everyone has the right to respect for his private and family life, his home and his correspondence*
>
> *ii) 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 or the economic wellbeing of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.*

1.2 It should be noted that Article 8 is a qualified right. If the right to respect for one's home private and family life is interfered with it has to be proportionate and in accordance with the exceptions in paragraph (ii).

1.3 Part 2 of RIPA provides a statutory framework that is compliant with the ECHR and provides guidance when using specified Surveillance techniques. It also introduces standards that apply to the police and other law enforcement agencies. Local authorities are classified as public bodies as their functions include the investigation of certain crimes. For example, the Council as a local authority investigate and prosecute:

(a) fraud;

(b) consumer protection offences (such as the sale of counterfeit and unsafe goods);

(c) noise nuisance; and

(d) non-compliance with planning enforcement notices.

These are just some examples of the myriad areas of enforcement the Council undertakes.

1.4 The Council can only use the provisions of RIPA in three areas - the acquisition and disclosure of communications data, the use of Directed Surveillance and covert human intelligence sources - for:-

'the purpose of preventing and detecting crime or preventing disorder'

1.5 The purpose of this policy is to provide guidance with regard to the use of Directed Surveillance, Covert Human Intelligence Sources (CHIS) and the acquisition and disclosure of Communications Data under RIPA. Covert Surveillance under RIPA requires internal authorisation as well as Court approval to reduce the risk of the information gathered being found to be inadmissible in court and/or expose the Council to liability for breach of Article 8.

1.6 The Investigatory Powers Act 2016 established the Investigatory Powers Commissioner's Office (IPCO). This organisation provides oversight of the use of investigatory powers by public authorities. The Council is subject to regular inspections by IPCO.

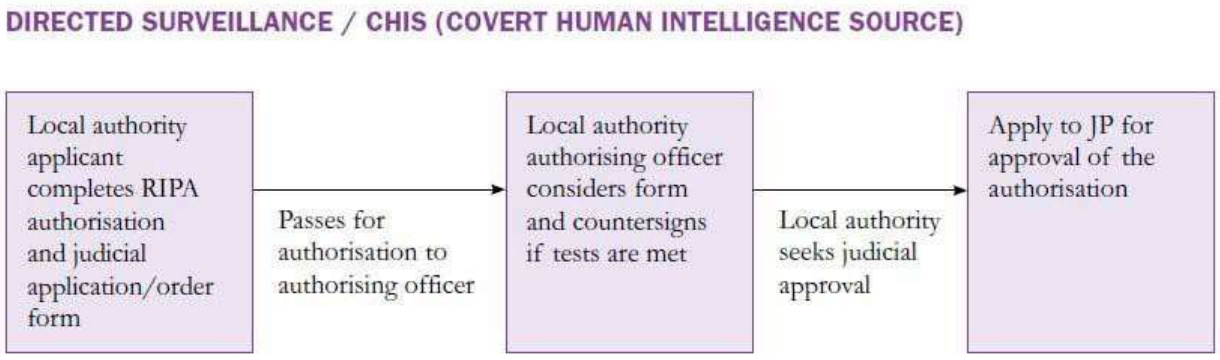
~~1.7~~ Codes of Pp~~p~~ractice have been drawn up by the Home Office and these are referred to at Appendix 1 but are not reproduced. They can be inspected at the Home Office website: ~~https://ww4w.gov.uk/government/collections/ripa-forms--2~~https://www.gov.uk/government/collections/ripa-codes

~~1.8~~1.7

~~1.9~~1.8 ~~Advice~~Guidance may also be obtained from the Home Office Codes of Practice on "Covert Surveillance and Property Interference" dated August 2018 and "Covert Human Intelligence Sources", ~~both~~ dated December 2022~~August 2018~~, and the "Acquisition and Disclosure of Communications Data" dated March 2015.

~~1.10~~1.9 This document applies to all Council staff and workers and to all contractors employed by the Council (all relevant Council contracts will include a term that this Policy and Guidance are to be observed by any contractor operating on behalf of the Council). Further it is important any Council officers satisfy themselves of the competence of any contractor to comply with RIPA and this Policy.

~~1.11~~1.10 From 1 November 2012 all authorisations and renewals under RIPA need court approval before they can come into effect. Such approval must be sought from a Justice of the Peace in the Magistrates' Court. The overall process is outlined below:



2. Key Terms

Key terms are defined and expanded upon here. These terms are capitalised throughout the document to indicate they have been defined in this paragraph.

2.1 "Authorising Officers"

Persons who have been trained to the appropriate level should be nominated as Authorising Officers. It will be the responsibility of these officers to

consider all RIPA applications and to grant or refuse authorisations, as appropriate. These Officers are central to the integrity of the process and it is vital that they understand their responsibilities being ultimately responsible to the Courts for the proper application of RIPA and this policy when considering requests for authorisation.

Under the Regulation of Investigatory Powers (Directed Surveillance and Covert Human Intelligence Sources) Order 2010 the prescribed officers are "Directors, Heads of Service, Service Managers or equivalent". Appendix 2 sets out the Authorising Officers for the Council.

However, when knowledge of Confidential Information is likely to be acquired or when a vulnerable individual or juvenile is to be used as a CHIS only the Head of Paid Service can authorise the relevant activity (or, in his or her absence, the person acting as the Head of Paid Service).

Authorisations (and renewals of authorisations) only come into effect if and when approved by an order of the Magistrates' Court (see Appendix 3).

Amendments to the list in Appendix 2 are to be agreed by the **RIPA Senior Responsible Officer**~~**/ RIPA Monitoring Officer**~~ (also defined in Appendix 2).

2.3 "Crime Threshold Test"

Directed Surveillance can only be used to prevent or detect criminal offences that are either:

- punishable, whether on summary conviction or indictment, by a maximum term of at least 6 months' imprisonment or
- an offence under:
  - section 146 of the Licensing Act 2003 (sale of alcohol to children);
  - section 147 of the Licensing Act 2003 (allowing the sale of alcohol to children);
  - section 147A of the Licensing Act 2003 (persistently selling alcohol to children);
  - section 7 of the Children and Young Persons Act 1933 (sale of tobacco, etc, to persons under eighteen).
  - Section 91 of the Children and Families Act 2014 (purchase of tobacco, nicotine products etc. on behalf of persons under 18)
  - Section 92 of the Children and Families Act 2014 (prohibition of sale of nicotine products to persons under 18)

This means, at the start of an investigation, Council officers will need to satisfy themselves that what they are investigating is a criminal offence falling into one of the above categories.

~~For investigations that do not meet the above criminal offence thresholds advice must be sought from the RIPA Coordinator on the potential use of a non – RIPA process.~~

2.4 "Collateral Intrusion"

Collateral Intrusion is where the investigation is likely to unexpectedly interfere with the privacy of individuals who are not covered by the authorisation. Applications for authorisation should include an assessment of the risk of any Collateral Intrusion.

2.5 "Confidential Information"

This has the same meaning as is given to it in sections 98 to 100 of the Police Act 1997.

It consists of matters subject to legal privilege, communications between Members of Parliament and another person on constituency matters, confidential personal information, or confidential journalistic material:

- Legal Privilege - includes both oral and written communications between a professional legal adviser and his or her client or any person representing his or her client, made in connection with the giving of legal advice to the client or in contemplation of legal proceedings and for the purposes of such.

Communication and items held with the intention to further a criminal purpose are not matters subject to legal privilege.

- Confidential Personal Information

"*Personal information*" means information concerning an individual (whether living or dead) who can be identified from it and relating--

(a) to his physical or mental health, or

(b) to spiritual counselling or assistance given or to be given to him.

"*Confidential Personal Information*" means personal information (as defined directly above):

(a) which a person has acquired or created in the course of any trade, business, profession or other occupation or for the purposes of any paid or unpaid office, and which he holds in confidence, and

(b) communications as a result of which personal information--

(i) is acquired or created as mentioned in paragraph (a), and

(ii) is held in confidence.

- Confidential Journalistic Material - includes material acquired or created for the purposes of journalism and held subject to an undertaking to hold it in confidence, as well as communications resulting in information being acquired for the purposes of journalism and held subject to such an undertaking.

Extra care should be taken in cases where the subject of the investigation might expect a degree of privacy or where Confidential Information is involved.

Officers should be aware of the requirement for authorisation where~~of such~~ Confidential or privileged Information is likely to be acquired can only be authorised by the Head of Paid Service. Advice should be sought from the Senior Responsible Officer~~and if any doubt to seek legal advice~~.

2.6 "Covert Human Intelligence Sources (CHIS)"

Under section 26(8) of RIPA a person is a covert human intelligence source if s/he establishes or maintains a personal or other relationship with a person for the covert purpose of facilitating:

(a) obtaining information;

(b) providing access to information to another person; or

(c) disclosing information obtained by the use of or as a consequence of such a relationship.

Surveillance by a human intelligence source is covert if:

- it is carried out in a manner calculated to ensure that persons who are subject to Surveillance are unaware that it is or may be taking place;

- if a relationship is established or maintained and then conducted in a manner calculated to ensure that one of the parties is unaware of the purpose; or

- any information obtained and disclosed is disclosed in a manner calculated to ensure that one of the parties to the relationship is unaware of the use or disclosure in question.

2.7 Covert Surveillance

Covert Surveillance is defined, under s26(9)(a) 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 categorised as either Intrusive or Directed.

2.8 Directed Surveillance

Directed Surveillance is defined in section 26(2) of RIPA as Surveillance which is covert, but not intrusive, and undertaken:

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

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

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

Directed 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 or associations. It does not include entry on or interference with property or wireless telegraphy (which the Council cannot do under RIPA), but may include the use of photographic and video equipment (including the use of CCTV).

2.9 "Intrusive Surveillance"

Intrusive Surveillance is defined in section 26(3) of RIPA 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 BUT Surveillance is not intrusive (but may still be directed) if it:-

(a) is carried out by a vehicle tracking device (s26(4)(a); or

(b) involves the consensual interception of mail or telecommunications for which there is no interception warrant (s26(4)(b); or

(c) involves a Surveillance device observing residential premises or a private vehicle, which device is not fitted in the premises or vehicle and which device does not consistently provide information of the quality and detail that would be obtained if the device was actually present on the premises or in the vehicle (s26(5).

A local authority officer cannot be authorised to conduct Intrusive Surveillance.

2.10 Interference with Property

Legal advice must be obtained in relation to the installation of surveillance equipment on private property to ensure that an officer does not inadvertently commit trespass

2.11 Core Functions of the Council

The 'core functions' referred to by the Investigatory Powers Tribunal (C v The Police and the Secretary of State for the Home Office IPT/03/32/H dated 14 November 2006) are the 'specific public functions', undertaken by a particular authority, in contrast to the 'ordinary functions' which are those undertaken by all authorities (e.g.employment issues, contractual arrangements etc.). A public authority may only engage the 2000 Act when in performance of its 'core functions'. The disciplining of an employee is not a 'core function', although related criminal investigations may be. ~~The protection of the 2000 Act may therefore be available in relation to associated criminal investigations so long as the activity is deemed to be necessary and proportionate. *For example A police officer claiming compensation for injuries allegedly sustained at work is suspected by his employer of fraudulently exaggerating the nature of those injuries. The police force of which he is a*~~

~~*member wishes to conduct covert surveillance of the officer outside the work environment. Such activity may relate to the discharge of the police force's core functions as the police force may launch a criminal investigation. The proposed surveillance is likely to result in the obtaining of private information and, as the alleged misconduct amounts to the criminal offence of fraud, a directed surveillance authorisation may be appropriate.*~~

2.11 "Judicial Approval"

The approval of Local Authority Authorisations under RIPA by a Justice of the Peace sitting in the Magistrates' Court (see Appendix 3)

2.11 "Private Information"

This includes, "in relation to a person", any information relating to his or her private or family life.

Aspects such as gender identification, name, sexual orientation and sexual life are important elements of the personal sphere protected by Article 8. The Article also protects a right to identity and personal development, and the right to establish and develop relationships with other human beings and the outside world and it may include activities of a professional or business nature. There is, therefore, a zone of interaction of a person with others, even in a public context, which may fall within the scope of "private life". It may be the case, therefore, that a person's private life may be concerned in measures affected outside a person's home or private premises. A person's reasonable expectations as to privacy are a significant though not necessarily conclusive factor.

2.12 "Surveillance"

Includes (under s48(2):

(a) monitoring, observing or listening to persons, their movements, their conversations or their other activities or communications;

(b) recording anything monitored, observed or listened to in the course of Surveillance; and

(c) Surveillance by or with the assistance of a device.

3. Directed Surveillance

3.1 General

3.1.1 In general terms, Directed Surveillance is planned covert Surveillance which could not be classed as Intrusive Surveillance. To fall into the category of Directed Surveillance, the Surveillance must be undertaken for the purpose of a specific investigation or operation in a way likely to obtain Private Information about a person (otherwise than by immediate response to events). If Surveillance takes place as an immediate response to an event, no authorisation is required. Directed Surveillance is essentially Surveillance carried out in a manner calculated to ensure that the person who is the subject of the Surveillance is unaware that it is, or may be, taking place. Thus for example plain clothed trading standards officers attending a car boot sale to generally observe for sale of counterfeit material, and then observed such a sale would be acting as an immediate response to events and would not be considered to be Directed Surveillance. However if they attended the car boot sale acting on intelligence that a specific trader was selling illegal goods and then proceeded to "target" that trader and observe them then that is likely to be considered "Directed Surveillance".

3.1.2 Directed Surveillance can only be used if authorised in accordance with this Policy and only then after the authorisation has been approved by an order of the Magistrates' Court

3.1.3 Directed Surveillance can only be used to prevent or detect criminal offences that meet the Crime Threshold Test

3.1.4 During the course of an investigation the type and seriousness of offences may change. The option of authorising Directed Surveillance is dependent on the offence under investigation meeting the Crime Threshold Test. Providing this is the case, an application for authorisation or approval can be made. However, if during the investigation it becomes clear that the activity being investigated does not amount to a criminal offence or that it would be a less serious offence that does not meet the threshold the use of Directed Surveillance should cease. If a Directed Surveillance authorisation is already in force it should be cancelled.

3.1.5 Directed Surveillance will be authorised against a specific offence which meets the threshold, and the type and the timing of the deployment of the Surveillance will always reflect this.

3.2 Further points on Directed Surveillance

~~3.2.1 A dog warden, who *happens* to see a dog fouling offence being committed, would not be said to be undertaking Directed Surveillance in the RIPA sense. To be planned Surveillance, there needs to be a specific purpose or investigation. (It's also unlikely this offence would meet the Crime Threshold Test.)~~

~~3.2.2~~3.2.1 If an investigating officer responds to an immediate event this would not be Directed Surveillance. If the officer subsequently planned a follow-up visit for the specific purpose of carrying out observations this would be classified as Directed Surveillance and would require authorisation.

~~3.2.3~~3.2.2 Directed Surveillance is usually undertaken by means of an individual officer watching or recording the person while they undertake or are suspected of undertaking the prohibited activity. It can also include an officer making a test purchase from a person when the transaction is captured on a recording device that may be worn by the officer. It is not necessary for the recording to be visual; an audio recording only would also be classed as Directed Surveillance. Evidence can also be gained by way of photography.

~~3.2.4~~3.2.3 Hidden cameras in a public place or targeted CCTV also constitute covert Surveillance. In such circumstances a CCTV camera is trained on a specific person or a spot at a particular time in order to observe the activities of a particular person or group of persons. That being said, where CCTV is used in the monitoring of public areas in an overt way i.e clearly signposted and just happen to catch a criminal act, this would **not** be classified as covert Surveillance.

~~3.2.5~~3.2.4 RIPA covers local authorities; therefore any contractor, employee or worker of the Council is covered. It does not include local authorities acting on information that is received from members of the public acting on their own volition. Officers should use this information to carry out their own investigation. Officers should not encourage the member of the public to continue providing further information, as they may unintentionally engage them as a Covert Human Intelligence Source (CHIS). ~~For example, neighbours filming nuisance activities across the road behind their net curtains and then giving the tape to Environmental Health for action or as evidence without being actively recruited to do so does not require authorization. However, such activity should not be encouraged by officers, as the neighbour may unintentionally act as a Cover Human Intelligence Source (CHIS).~~

~~3.2.6~~3.2.5 A public authority may only engage RIPA when in performance of its 'core functions' – i.e. the 'specific public functions', undertaken by a particular authority, in contrast to the 'ordinary functions' which are those undertaken by all authorities (e.g. employment issues, contractual arrangements etc) see *C v The Police and the Secretary of State for the Home Office* – IPT/03/32/H). The disciplining of an employee is not a 'core function', although related criminal investigations may be.

~~3.2.7~~3.2.6 More details are set out in the Council's relevant employment policies.

Examples of Directed Surveillance by local authority investigators

(a) a recorded test purchase such as a suspected pirate DVD or counterfeit goods being purchased from a market trader.

(b) the training of a CCTV camera onto a particular trading premises to establish who opens and closes the premises each day.

~~(c) observing of persons suspected of serious or serial benefit fraud to see if they are going to and from a place of work~~

(c following of a person suspected of dangerous waste dumping.

~~(e) the taping of nuisance tenants (to measure the level of sound) by Housing Officers or contractors engaged by them for the purposes set out in the Anti-Social Behaviour Act 2003. However, this is normally carried out overtly by advising the subject via letter or notice in advance in which case an authorisation would not be applicable~~

Activities such as the test purchasing of alcohol and cigarettes by underage persons need to be considered on a case- by-case basis.

3.2.83.2.7 Examples of what does not constitute Directed Surveillance:

- "Hot spot targeting" e.g. licensing officers standing on a street to monitor private hire cars plying for hire illegally where this is not part of a planned operation, or Surveillance on a fly-tipping ~~or a dog-fouling clear up~~.

- Overt CCTV or Surveillance by way of an immediate response to events.

- Overt investigations, e.g. an Environmental Health Office ~~Benefits Officer~~ visiting a person to make enquiries and declaring their status and intention ~~or Environmental Health Officers declaring their status and intention.~~

-

4. Covert Human Intelligent Sources (CHIS) URGENT ADVISE MUST BE SOUGHT AS FROM THE RIPA COORDINATOR IF CHIS IS BEING CONSIDERED

4.1 A CHIS is a person who establishes or maintains a personal relationship or other relationship with a person in order to covertly obtain or disclose information (Section 26 (8) (a) to (c) of RIPA). The code of practice recognises CHIS as agents, informants or officers working under cover. In the case of a local authority a CHIS would normally be an informant or an officer working under cover.

4.2 As with covert Surveillance, a CHIS would not be a member of the public who volunteers information to the local authority, such as a person who complains that they purchased food past its use-by date from their local supermarket. In this case the relationship between customer and provider is too remote. It should also be considered that the information may well be given ~~secretly~~ confidentially and may not be revealed to the defendant as it may be deemed to be sensitive in accordance with the Criminal Procedure and Investigations Act 1996. It should also be borne in mind that an informant may well be providing regular information during an investigation, and if requested to continue to do so will be a CHIS whereas a member of the public complaining is usually a one-off incident and will not be a CHIS.

~~4.3~~ The rules of evidence permit investigators to use ruses to gain information provided that the person is not persuaded into committing an unlawful act that they otherwise would not have committed. For example trading standards officers may masquerade as members of the public when visiting a car dealer and may pose questions that a prospective customer might well ask and in doing so may well gain information. In such cases this officer would be a CHIS as they would be deemed to be an officer working under cover and could be seen to be seeking to gain a person's trust. An officer who merely goes into a shop and purchases an item without engaging in dialogue except for, 'how much?' and 'thank you', would not be a CHIS. Although in this circumstance the officer is working under cover, they are not seeking information from that person or intending to gain that person's trust. ~~In extreme situations, trading standards officers and police have gone under cover and worked in establishments to gain information.~~

~~4.4~~4.3

~~4.5~~4.4 It should be noted that an officer who attends a premises and identifies him/herself and then either carries out a statutory inspection or has entered in pursuance of a warrant of entry issued by a court, is not a CHIS. There is nothing covert about their visit.

~~4.6~~4.5 The use and/or conduct of a CHIS must be authorised internally (see paragraph 7 below). Further, such an authorisation can only come into effect once approved by an order of the Magistrates' Court (see Appendix 3).

Additional Considerations when using a CHIS

4.74.6 If a CHIS is a juvenile or a vulnerable person the authorisation can only be given by the Chief Executive (as Head of Paid Service) (see Appendix 2).

4.8 Furthermore, the Council must have arrangements in place for ensuring that there will be at all times a person holding a position or office within the Council who will have day to day responsibility for dealing with the CHIS on behalf of the Authority. This will include the CHIS's security and welfare. They are known as a "Handler". In addition to this person, the Council must also ensure that there will be at all times another person who will have general oversight of the use made of the CHIS (known as a "Controller"). It is suggested that the former is the officer having responsibility for the general management of the case and the latter is the appropriate Authorising Officer.

4.8A It is particularly important that before authorising use of a CHIS, that the Authorising Officer ensures that a risk assessment has been carried out with respect to an risk to the security and welfare of the CHIS, and others who may be foreseeably affected by the operation. This extends to the assessment of any risk that may exist after the cancellation of the authorisation and must include the management of any requirement to disclose the existence or identity of the CHIS in any subsequent legal proceedings.

4.8B As the CHIS activity continues the remit of the authorisation and the risk assessment must be kept under regular review, this is the primarily the responsibility of the "handler". Any activity outside of the authorisation and / or any need to extend the remit must be reported to the Authorising Officer. If the remit needs to be extended then this can only be done via judicial approval.

4.8C A CHIS may be authorised to use or have a covert recording device on their person. This is generally permissible subject to the usual considerations of proportionality. A CHIS wearing or carrying a surveillance device does not need a separate directed surveillance authorisation, provided the device will only be used in the presence of the CHIS. However, if a surveillance device is to be used other than in the presence of the CHIS, directed surveillance authorisation should be obtained where appropriate, together with an authorisation for interference with property, if applicable. See the Covert Surveillance and Property Interference Code of Practice.

4.8D There must be a centrally retrievable record of CHIS authorisations containing only*:*

a) The name, or the code name, of the Unique identifying reference of the CHIS
b) Dates of the authorisation / renewal and cancellation of the CHIS
c) Whether the CHIS is "self-authorised" (which is very unlikely in the circumstances of a local authority)

These records must be held for 5 years from the date that the authorisation ends.

4.9 Separately other records must be held with reference to the individual authorisation. The officer in charge of maintaining a record of the use of a CHIS must also, at all times, record the following particulars as specified by the Secretary of State:

(a) The identity of the CHIS.

(b) The identity, where known, used by the CHIS.

(c) Any relevant investigating authority other than the authority maintaining the records.

(d) The means by which the source was referred to within each relevant investigating authority.

(e) Any other significant information connected with the security and welfare of the CHIS.

(f) Any confirmation made by the Authorising Officer for the conduct or use of a CHIS that the information in paragraph 5 above has been considered and that any identified risks to the security and welfare of the CHIS have, where appropriate, been explained to and understood by the CHIS.

(g) The date when and the circumstances in which the CHIS was recruited.

(h) The identities of the Authorising Officer and the officer who applied for the use of the CHIS.

(i) The periods during which those persons have discharged those responsibilities.

(j) The tasks given to the CHIS and the demands made of him/her in relation to his/her activities as a CHIS.

(k) All contacts or communications between the CHIS and a person acting on behalf of any relevant investigating authority.

(l) The information obtained by each relevant investigating authority by the conduct or use of the CHIS.

(m) Any dissemination by that authority of information in that way.

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

4.10 In addition the records or copies of documents required by paragraph 7.6 of the CHIS/COP should be retained for 5 years.

4.11 The intention is that adequate records must be kept in such a way that the CHIS is safe from discovery by the subject(s) of the investigation and safe from any harm which could result from a disclosure of information. Further, it is meant to keep in the open any money or benefits paid to the CHIS who is not employed by the Council. See paragraph 12.5 for further requirements in relation the use of a CHIS.

5. Necessity and Proportionality

5.1 When engaging in covert Surveillance, including use of a CHIS, the most likely Article of the ECHR to be breached is Article 8 referred to in paragraph 1.1 above. This is a qualified right and can be interfered with, if:

(a) the aim of such interference is **necessary** for the purpose of preventing and the detection of crime or preventing disorder (see paragraph 7.2 below); and

(b) the covert activities are **proportionate** in the circumstances of the particular case.

5.2 The Authorising Officer must be satisfied that the use of covert surveillance is necessary for one of the purposes specified in section 28(3) of RIPA. In order to be satisfied, the conduct that it is aimed to prevent or detect must be identified and clearly described, particularly if it is questionable whether serious crime criteria are met. ~~Often missed is an~~The authorisation form will record the explanation of why it is considered necessary to use the covert techniques requested

5.3 Proportionality is a key concept of RIPA. ~~It is often poorly articulated.~~ An authorisation should demonstrate how an Authorising Officer has reached the conclusion that the activity is proportionate to what it seeks to achieve; including an explanation of the reasons why the method, tactic or technique proposed is not disproportionate (the proverbial 'sledgehammer to crack a nut'). Proportionality is not only about balancing the effectiveness of covert methods over overt methods but of explaining why the particular covert method, technique or tactic is the least intrusive. It is insufficient to make a simple assertion or to say that the 'seriousness' of the crime justifies any or every method available. It may be unacceptable to advance lack of resources or a potential cost saving as sufficient ground to use technological solutions which can be more intrusive than a human being. This critical judgment can only properly be reached once all other aspects of an authorisation have been fully considered.

The following elements of proportionality ~~had been~~should be fully considered:

- balancing the size and scope of the operation against the gravity and extent of the perceived mischief
- explaining how and why the methods to be adopted will cause the least possible intrusion on the target and others
- that the activity is an appropriate use of the legislation and the only reasonable way, having considered all others, of obtaining the necessary result, and
- providing evidence of other methods considered and why they were not implemented.

5.3 Covert Surveillance should therefore be used as a last resort.

6. Covert surveillance of Social Networking Sites (SNS)

6.1 The OSC Procedures and Guidance 2016 states: 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.

6.2 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.

6.3 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).

6.4 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 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.

6.5 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).

7. General Provisions about Authorisations

7.1 Where an investigating officer of the Council wishes to engage in covert Surveillance, or wishes to either operate as or use a CHIS, RIPA sets out procedures for who can provide authorisatione and what the evidence obtained is to be used for. In order to perform covert Surveillance or to operate/use a CHIS, the officer who wishes to do so must obtain:

Step 1: **authorisation** by the appropriate nominated officer ('Authorising Officer') (See Appendix 2),

Step 2: **approval** of the authorisation by the Magistrates (See Appendix 3)

7.2 Surveillance must only be authorised where it is believed that the Surveillance is necessary under the ground set out in paragraph 7 and is proportionate to what it seeks to achieve. To protect privacy, and comply with the HRA, all Council services will need to demonstrate that any intrusion into an individual's privacy is essential to an investigation.

7.3 Where Surveillance is considered appropriate it must still be authorised and then approved by an order of the Magistrates' Court before it can commence.

7.4 Authorising Officers will need to satisfy themselves that a defensible case can be made for Surveillance activity. The matters which the Authorising Officer must consider are set out in Section 8 below. Obtaining an authorisation and Magistrates' approval will ensure that the action is carried out in accordance with the law and subject to stringent safeguards against abuse. It will also make the action less vulnerable to challenge under the HRA

7.5 Where an authorisation is approved for Directed Surveillance / CHIS then it must only be carried out in accordance with the authorisation and only for the purposes of the investigation specified or described. It is also vital that the remit of the authorisation is communicated to and understood by, the Surveillance officers or the CHIS.

7.6 In no circumstance must any Covert Surveillance operation be given backdated authorisation after it has commenced. Embarking upon Directed Surveillance or the use of a CHIS without court-approved authorisation or conducting Covert Surveillance outside the scope of the authorisation will mean that the 'protective umbrella' of RIPA is unavailable and so any evidence obtained is likely to be inadmissible in court. This may also result in disciplinary action being taken against the officer/officers concerned within the Council's Human Resources policies and procedures.

8. Grounds for Authorisation

8.1 Authorisation for Directed Surveillance or the use of a CHIS may be granted by an Authorising Officer where and only where s/he believes:-

(a) that the authorisation is necessary for the purpose of preventing and detecting crime or preventing disorder; and
(b) that the authorised Surveillance is proportionate to that which is sought to be achieved (see paragraph 5).

8.2 Authorisation for using a CHIS can only be given for preventing or detecting crime or of preventing disorder.

8.3 Authorisation for Directed Surveillance can only be given for preventing or detecting criminal offences that meet the Crime Threshold Test. Directed Surveillance **cannot** be used for offences below that threshold or to prevent disorder.

8.4 Detecting crime includes establishing by whom, for what purpose, by what means and generally in what circumstances any crime was committed, the gathering of evidence for use in any legal proceedings and the apprehension of the person (or persons) by whom any crime was committed. Preventing or detecting crime goes beyond the prosecution of offenders and includes actions taken to avert, end or disrupt the commission of criminal offences.

8.5 In the case of crime when the investigator comes to the Authorising Officer the latter will be hard pressed, in many cases, to know whether s/he is satisfied that the investigation will follow the criminal route. If the concern is disorder this problem is greatly reduced since the evidence is being gathered to be presented for a wide range of remedies. Thus use of a CHIS under RIPA can be used in cases where disorder is being alleged under the Anti-Social Behaviour Act 2003.

9 Completing the Forms for Authorisation

9.1 The investigating officer seeking authorisation does this by completing the necessary form. To ensure that the current forms are being used, they should be downloaded from the Home Office Website each time a new Authorisation is being sought at https://www.gov.uk/government/collections/ripa-forms--2

When completing these forms for authorisation, they should provide:

- Name(s) (where known) or description(s) of the person(s) who is/are to be the subject of the Surveillance as well as any known history and character of that/those person(s).

- The location of the person who is the subject of the Surveillance or where such Surveillance is to take place and (if relevant) the place where the CHIS is to be located.

- The type of Surveillance device or equipment to be used (if any).

- The type of activities, numbers and names of officers who will be CHIS's (if relevant).

- The purpose of which the Surveillance is to be undertaken or CHIS used. As stated above, it also has to be demonstrated why it is necessary to use covert Surveillance or a CHIS.

- It must specify why the Surveillance to be undertaken or CHIS used is proportionate and in this context specifying:

  (a) The objectives of the Surveillance or the use of the CHIS

  (b) The crime or disorder being investigated

  (c) Why the Surveillance or the use of a CHIS should be used in preference to other methods of investigation

  (d) Why it would be more practicable

- For Directed Surveillance, confirmation that the criminal offence(s) (which should also encompass any "disorder") meet the Crime Threshold Test, and brief details in support of this confirmation.

- The objectives of the activities.

- The name and nature of the investigation or operation and what makes the Authorising Officer believe Surveillance or the use of the CHIS will achieve the objectives.

- The risk of information relating to third parties' private and family lives being obtained i.e. Collateral Intrusion.

- The likelihood of acquiring any confidential/religious material.
- The period of review that will apply
- Whether the Authorisation was ultimately refused and reasons why

10. Duration of Authorisations

(a) Time Limits

10.1 Authorisations have a duration as follows:

• Directed Surveillance	3 months from grant of judicial approval
• Covert human intelligence source (where CHIS 18 or older)	12 months from grant of judicial approval
• Covert human intelligence source (where CHIS under 18)	1 month from grant of judicial approval

and will cease to have effect after these periods. However, the authorisations will continue to exist until cancelled. The process of controlling RIPA authorisations should be by review and cancellation. If they are no longer required they should be cancelled proactively and not simply allowed to expire.

(b) Review

10.2 Once granted, an authorisation should be reviewed regularly, at least as required by the Authorisation, by the officer managing the case to assess whether or not the activity authorised continues to be **necessary** and **proportionate**. The Authorising Officer should be notified of any instances where these criteria are no longer met. Reviews should be more frequent when access to Confidential Information or Collateral Intrusion is involved. Review frequency should be as often as the Authorising Officer deems practicable. Judicial approval is not required for an internal review.

10.3 The Authorisation forms should be used in conducting a review of Covert Surveillance or a CHIS.

(c) Renewal

10.4 If at any time before an authorisation would cease to have effect the Authorising Officer considers it necessary for the authorisation to continue for the purpose for which it was given, they may renew it in writing for a further period not exceeding the relevant time limits in paragraph 10.1. Once authorised, renewals must also be approved by the Magistrates' as with initial authorisations (see Appendix 3).

10.5 A renewal takes effect at the time at which, or day on which the authorisation would have ceased to have effect but for the renewal. An application for renewal should not be made until shortly before the authorisation period is drawing to an end. Any person who would be entitled to grant a new authorisation can renew an authorisation. Authorisations may be renewed more than once, provided they continue to meet the criteria for authorisation.

10.6 An application for renewal should be made to the officer who granted the original authorisation unless there is a very good reason not to do so (e.g. because the original Authorising Officer is on annual leave/ has left the Council).

10.7 Applications for renewal should be made using the forms contained in Appendices 4

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

(d) Cancellation

10.9 Finally with regards to authorisations, an authorisation must be cancelled by the person who granted or renewed it if that person is satisfied that the authorisation is no longer necessary on the ground under which it was granted or renewed or it is no longer proportionate to what is sought to be achieved by carrying it out. Alternatively, in the case of the authorisation of a CHIS, that person is satisfied that arrangements for the CHIS's case that satisfy the requirements as set out above no longer exist. When cancelling, the forms contained in Appendices 4 and 5 should be used. Judicial approval is not needed for a cancelation.

11 RIPA Coordinating Officer and Record Keeping

11.1 The RIPA Coordinating Officer will keep this Policy and Guidance document under review and will amend it to accord with best practice. They will also hold a centrally retrievable record of all authorisations and regularly update it whenever an authorization is granted, renewed or cancelled. The record will be made available to an Inspector from the Investigatory Powers Commissioner's Office, upon request. The record will be retained for a period of at least five years from the ending of the authorisation and will contain the following information:

- the type of authorisation;
- the date the authorisation was given;
- name and rank of the Authorising Officer;
- the unique reference number (URN) of the investigation or operation;
- the title of the investigation or operation, including a brief description and names of subjects, if known;
- Length of the Authorisation
- Review Periods

- if the authorisation is renewed, when it was renewed and who authorised the renewal, including the name and rank of the Authorising Officer;

- whether the investigation or operation is likely to result in obtaining Confidential Information as defined in this code of practice;

- the details and outcome of applications to the Magistrates' for judicial approval, including names of Magistrates and dates and times of hearings

- the date the authorisation was cancelled.

11.2 All original authorisations, renewals and cancellations shall be held by the RIPA Coordinating Officer with copies held by the Authorising Officer. These will include:

- a copy of the application and a copy of the authorisation together with any supplementary documentation and notification of the approval given by the Authorising Officer;

- a copy of the court order approving the authorisation

- 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;

- the date and time when any instruction was given by the Authorising Officer.

- The Cancellation Form

12 Record Keeping – Generally

12.1 Copies of all written authorisations and reviews should be kept for a period of five years from the ending of the Authorisation or longer if required by the Criminal Procedure and Investigations Act 1996..

12.2 All information that is obtained during Surveillance undertaken for the purpose of a criminal investigation is recorded by means of a Surveillance log. This log should give an account of the events observed and conversations heard and the time and date of such events or conversations. As it is unlikely that such a log would be completed contemporaneously, the date and time that the entry is made should also be noted as well as the name of the person making the entry.

12.3 Where an authorisation is reviewed and either granted, withdrawn or refused then the review must be recorded in writing on the relevant form.

12.4 At no time must any of the recorded information be disclosed or used, except for the purposes for which it was gathered at that time or for use in any future criminal or civil proceedings involving the Council, or if disclosure is required by law.

12.5 All reference to the CHIS must be by way of the pseudonym or URN allocated. The only document that records the true identity of the CHIS is the 'source profile' which must be securely stored away from all other operational documentation. All of the information obtained by a CHIS and by the officer responsible for recording the use of the CHIS is to be recorded in a daily log similar to that referred to above for Surveillance. Where such a log also reveals the name of the CHIS this should only be disclosed if either legally necessary or if required by a Court. See paragraphs 4.6 to 4.10 for further requirements in relation to the use of a CHIS. Material produced by Covert Surveillance and use of CHIS will be retained in accordance with law, such as the requirements of the Criminal Procedure and Investigations Act 1996.

12.6 The Freedom of Information Act 2000 (FOIA) provides for the general rights of access to recorded information held by public authorities and specifies the conditions before a request has to be complied with. The advice of the RIPA Coordinating Officer should be sought for any requests to see the authorisation documents under the FOIA.

13 Use of Covert Surveillance equipment, data security and data sharing

13.1 Covert Surveillance equipment will only be installed with the necessary authorisation of the Council's Authorising Officers and only then when that authorisation has been approved by the Magistrates'. It will only be installed in residential premises if a member of the public has requested help or referred a complaint to the Council and such matter can only be investigated with the aid of Covert Surveillance techniques. Any permission to locate Surveillance equipment on residential premises must be obtained in writing from the householder or tenant, and should encompass all occupiers of the premises.

13.2 In the unlikely event ~~Any request by~~ a Council officer requests~~to~~ a resident to keep a video/audio/written diary as part of a covert evidence-gathering exercise this will be regarded as a Covert Surveillance exercise conducted on behalf of the Council and must be authorised and judicially approved in accordance with this policy.

13.3 During a covert operation, recorded material or information collected will be stored and transported securely. It will be reviewed daily and access to it will be restricted to the investigating officers and the Authorising Officer concerned. The RIPA Monitoring and Coordinating Officer will decide whether to allow requests for access by third parties including other Council officers. Access will generally only be allowed to limited and prescribed parties, including law enforcement agencies, prosecution agencies, legal representatives and the people subject to the Surveillance (unless disclosure would prejudice any criminal enquiries or proceedings). Requests for access will be dealt with in accordance with the Data Protection Act 1998.

13.4 A register will be maintained by the Authorising Officers of all reviews of material recorded and collected covertly.

13.5 Only high-quality digital or other recordings will be used. All DVDs and audiotapes will be identified uniquely. A register will be kept of all DVDs used to control the period of time they are retained (31 days) if not required for evidential purposes and the number of times they are re-used before being destroyed.

13.6 A register of recording and other surveillance equipment should be maintained to include details of its use.

14 Closed Circuit Television (CCTV)

14.1 Slough Borough Council is committed to respecting people's rights to privacy and supports the individual's entitlement to go about their lawful business; this is a primary consideration in the operation of any CCTV system operated by the council. Other agencies can request the use of public space CCTV systems for operational purposes, where RIPA applies, a copy of the RIPA authorisation will be held by the RIPA coordinator.

14.2 The Council uses secure video imaging systems (CCTV) in public spaces, within car parks and at a number of council owned and operated sites operated sites across the borough. CCTV in these areas is usually clearly sign-posted and visible.

14.3 The Council's CCTV policy at:

http://www.slough.gov.uk/crime-prevention-and-emergencies/cctv.aspx

covers the purchase and use of CCTV equipment and includes the use of cameras for RIPA purposes.

15 The "Policing" of RIPA

15.1 RIPA is overseen by the Investigatory Powers Commissioner's Office. They are tasked with ensuring that RIPA is being applied properly. Inspections can be carried out at regular intervals.

15.2 In addition, any person aggrieved by the way a local authority carries out covert Surveillance can apply to The Investigatory Powers Tribunal for redress, within a year of the act complained of or any longer period that the Tribunal thinks it just and equitable to allow. This Tribunal can quash any authorisation and can order the destruction of information held or obtained in pursuit of it. It can award compensation, but its findings may be of use in a Human Rights case challenge or as a defence to a case brought by the Council or in a referral to the Local Government Ombudsman or a complaint to the Information Commissioner, from where compensation awards can flow.

16 Consequences of Non Compliance

16.1 Where covert Surveillance work is being proposed, this Policy and Procedural Guidance should be strictly adhered to in order to protect both the Council and individual officers from the following:

(a) **Inadmissible Evidence** - there is a risk that, if Covert Surveillance and Covert Human Intelligence Sources (both defined at paragraph 2) are not handled properly, the evidence obtained may be held to be inadmissible.

(b) **Legal Challenge** – as a potential breach of Article 8 of the European Convention on Human Rights, which establishes a "right to respect private and family life, home and correspondence", incorporated into English Law by the HRA. This could not only cause embarrassment to the Council but any person aggrieved by the way it has carried out Covert Surveillance can apply to The Investigatory Powers Tribunal under RIPA for redress within a year of the act complained of or any longer period that the Tribunal thinks it just and equitable to allow. This Tribunal can quash any authorisation and can order the destruction of information held or obtained in pursuit of it. Its findings may be of use in a Human Rights case challenge, as a defence to a case brought by the Council, in a referral to the Local Government Ombudsman or a complaint to the Information Commissioner from where compensation awards can flow.

(c) **Censure** – the Investigatory Powers Commissioner's Office conduct regular audits on how local authorities implement RIPA. If it is found that a local authority is not implementing RIPA properly then this could result in censure and reputational damage.

(d) **Disciplinary Action** – failure of officers to comply with this Policy and Procedural Guidance may be regarded as a disciplinary offence under the Council's Disciplinary Policies and Procedures.

17. Complaints Procedures

17.1 The Council's Complaints Procedure should be used for any complaint, regarding breach of this Policy and Guidance.

17.2 Contravention of the Data Protection Act 1998 should be reported to the Head of Paid Service and the Information Commissioner,

18. The Role of Elected Members

Elected members are responsible for setting and reviewing the Council's policy and should not be involved in the authorisation of individual cases. Cabinet should receive a report at least annually on activity in the last year, a formal review of the policy and recommendations of any amendments. ~~of a local authority have the following responsibilities with regard to RIPA which rests primarily with the Commissioner for Regulation & Consumer Protection :~~

~~The Commissioner :~~

~~should review the authority's use of RIPA and present an annual report to Cabinet~~

~~should seek endorsement from Cabinet to set the policy at least once a year;~~

should consider internal reports on the use of RIPA on at least a quarterly basis to ensure that it is being used consistently with the local authority's policy and that the policy remains fit for purpose;

should not be involved in making decisions on specific authorisations.

19.1 RIPA ~~Monitoring~~ Senior Responsible Officer

The Monitoring Officer of the Council is the Senior Responsible Officer [SRO] and is responsible for:-

- the integrity of the process;
- compliance with Act and Code;
- oversight of reporting errors and reasons; and
- facilitating inspections.

19.2 The RIPA Coordinating Officer has responsibilities for –

- ensuring that all Authorising Officers are of an appropriate standard;
- addressing any concerns about the standards of Authorising Officers;
- the integrity of the processes in place for the management of CHIS and Directed Surveillance authorisations;
- compliance with RIPA and with the Codes;
- oversight of the reporting of errors to the IPCO etc;
- engagement with the IPCO when they conduct their inspections;
- where necessary, oversight of the implementation of post-inspection action plans approved by the IPCO

20. Communications Data

This aspect of the manual sets out the Council's policies, procedures and Codes of Practice regarding the acquisition of communications data (Comms Data). Designated Officers for Comms Data purposes are detailed at Appendix 5

In all cases applications for Comms data will be made through the National Anti Fraud Network (NAFN). NAFN submit applications on behalf of the Council to the Office for Communications Data Authorisations (OCDA)

The application of the procedures in this section is mandatory for all Council service areas that undertake these functions. This Section has been revised following changes introduced by the Investigatory Powers Act 2016 and should be read in conjunction with the **Home Office Acquisition & Disclosure of Communications Data Code of Practice**. https://www.gov.uk/government/publications/code-of-practice-for-the-acquisition-and- disclosure-of-communications-data

20.1 LAW & PROCEDURE

What is Comms Data?

The term 'communications data' embraces the 'who', 'when', 'where', and 'how' of a communication but not the content, not what was said or written.

Communications data is broadly split into three categories:

1. service data i.e. the use made of the service by any person, for example, itemised telephone records;

2. subscriber data i.e. any other information that is held or obtained by an operator or a person to whom they provide a service, for example, who the subscriber is of a telephone number or who the account holder is of an email address

3. traffic data i.e. where a communication was made from, to whom and when

The Investigatory Powers Act 2016 provides that a Council can obtain authorisation for the acquisition and disclosure of communications if three criteria are met:

1. it is necessary for the Council to obtain communication data for an applicable crime purpose in relation to a specific investigation;
2. the Council is party to a collaboration agreement certified by the Secretary of State;
3. the conduct to be authorised is proportionate to what is sought to be achieved.

20.2 <u>Basis for lawful acquisition of data</u>

Local Authorities are permitted in limited circumstances to obtain communications data, which would result in the subject's Right to Privacy being infringed.

Part 3 of the Investigatory Powers Act 2016 provides the statutory framework to enable the acquisition of communications data to be lawfully authorised and conducted so as to ensure it is compatible with **Article 8**.

20.3 <u>What are Local Authorities permitted to obtain?</u>

The Council is only permitted to access subscriber information and service data. The Council cannot access traffic data. The Council can only request subscriber information or service data if it is required for the purpose of preventing or detecting crime or protecting public health. Such a request must be both necessary and proportionate as discussed previously in this policy. The Council is not permitted to intercept the content of communications.

Failure to satisfy legislation – consequences

Please see paragraph **16~~15~~**

20.4 Slough's Centralised System

As detailed in para 11~~10~~ and 19~~18~~ The RIPA Co-ordinating Officer is responsible for maintaining a register of RIPA applications. All officers must discuss the intention of applying for a RIPA authorisation and once agreed the investigating officer must obtain a URN before progressing with the application. It is the responsibility of the applying officer to provide details to the RIPA Coordinating Officers team on progress of the RIPA authorisation application, use and if appropriate renewal and revocation. Refer to Quick Guide and flow chart on page 34.

20.5 Forms to be Used

Applications for Comms data are made on line via the NAFN portal

20.6 Relevant Definitions

a) Single Point of Contact [SPOC]

SPOCs are an accredited individual or group trained to facilitate the lawful acquisition of communications data and effective co-operation between a public authority and a CSP. For all Comms Data applications the Council uses NAFN SPOCs.

b) CSP

An operator who provides postal or communications data is described as a communications service provider [CSP].

The Council uses the NAFN service and officers are required to consult a NFN SPOC throughout the application process. The SPOC will scrutinise the application and if he/she agrees the application is lawful, will submit the application to the Office for Communications Data Authorisations on behalf of the Council.

20.7 Disclosure Duties & Procedure

a) Please see paragraph 19 above.

b) Original Application

To be retained by the SPOC

c) Golden Copy

Any documents or material provided to the Commission by a CSP as a result of a RIPA enquiry must be retained. This material is referred to by IOCCO as the 'Golden Copy' and this should always be available to be adduced in future legal proceedings if required. This is particularly important as the CSP may not retain the original data, depending on their retention policy.

20.8 Central Retrievable Record of Authorisations & Notice

Trading Standards maintain an Electronic Central Retrievable Record of Authorisations and Notices, which may be via NAFN

20.9 Senior Responsible Officer

T**he Regulation of Investigatory Powers (Directed Surveillance and Covert Human Intelligence Sources) Order** came into force along with an updated version of the Home Office's COP on 6th April 2010, which contained a mandatory requirement to appoint a Senior Responsible Officer. (The Senior Responsible Officer at Slough Borough Council for Comms Data is the Group Manager – Consumer Protection))

The Senior Responsible Officer [SRO] must be responsible for:-

. the integrity of the process;
. compliance with Act and Code;
. oversight of reporting errors and reasons;
. facilitating inspections.

20.10 Recordable Errors

Each public authority has a duty to keep a log of recordable errors. The record will be maintained by the ~~Monitoring~~Senior Responsible Officer.

The following are Reportable Errors:-

- An authorisation or notice made for a purpose, or for a type of data, which the relevant public authority cannot call upon, or seek, under the Act;
- human error, such as incorrect transposition of information from an application to an authorisation or notice
- disclosure of the wrong data by a CSP when complying with a notice;
- acquisition of the wrong data by a public authority when engaging in conduct specified in an authorisation;

20.11 Training & Monitoring

~~In order to be a DP all officers must have attended a suitable training course and be accredited as such. Thereafter the SRO should ensure that all DP's receive regular updates and training as and when required.~~ All officers utilising RIPA for the acquisition of communications data must also have attended a suitable training course.

20.12 Oversight

The Investigatory Powers Commissioners Office oversees the acquisition of communications data.

20.13 Codes of Practice

Home Office Acquisition of Communications Data to be accessed via the following link:- https://www.gov.uk/government/publications/code-of-practice-for-the-acquisition-and-disclosure-of-communications-data

APPENDIX 1

All codes of practice are available using the following link:

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

All documents relating to RIPA forms are available using the following link:

https://www.gov.uk/government/collections/ripa-forms--2

Also, see the Home Office guidance to local authorities in England and Wales on the judicial approval process for RIPA and the crime threshold for Directed Surveillance. This is available on:

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

APPENDIX 2

DESIGNATION OF AUTHORISING OFFICERS

The following Authorising ~~o~~Officers are designated by the Council to authorise, renew and cancel Directed Surveillance or the use of covert human information sources (CHIS):

- Monitoring Officer (SRO)
- Head of Legal~~.~~
- Associate Director – Community and Public Protection
- Group Manager – Community Safety, Housing Regulation & Enforcement (Co-ordinating Officer)
- Corporate Fraud Manager

~~Title of Officer~~	~~Service Area~~
~~Director of Adults & Communities~~	~~Enforcement of housing and council tax benefits including the investigation of fraud in connection therewith~~
~~Director Children, Learning & Skills Services~~	~~All matters involving financial irregularity (excluding housing and council tax benefits) and issues relating to employees and workers.~~
~~Director of Transformation.~~	~~Planning and building control, environmental health and trading standards~~
~~Head of Legal Services~~	~~All other service areas~~
~~Chief Executive - Head of Paid Service (or in absence chief officer)~~	~~Authorisation of a juvenile or vulnerable person as a CHIS and where the obtaining of Confidential Information is likely.~~

The above officers are appointed and designated **Authorising Officers** under the Regulation of Investigatory Powers (Directed Surveillance & Covert Human Intelligence Sources) Order 2010.

The RIPA Senior Responsible Officer is the Council's Monitoring Officer~~Director of Finance & Resources~~

~~The RIPA Monitoring Officer is the Council's Monitoring Officer~~

The RIPA Coordinating Officer is the Group Manager – Community Safety, Housing Regulation and Enforcement~~Service Lead – Regulatory Services~~

The Council also designate the named officers' successors where they are responsible for the service area and have received Council training in the use of RIPA.

APPENDIX 3

Judicial Approval

a) Officers wishing use Directed Surveillance or a CHIS first need to obtain internal authorisation in accordance with this Policy. However **an authorisation does not take effect unless and until it has been approved by a Justice of the Peace** (JP) (i.e. a District Judge or lay magistrate). If at the hearing the JP is satisfied that the statutory tests have been met and that the use of the technique is necessary and proportionate he/she will issue an order approving the grant or renewal for the use of the technique as described in the application.

b) The hearing will not be in open court, and no press, public, the subject of the investigation or the subject's legal representative will be present. 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.

Making the Application

c) The flowchart below outlines the procedure for applying for judicial approval. Following approval by the Authorising Officer 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.

d) The Council will provide the JP with a copy of the original RIPA authorisation or notice and the supporting documents setting out the case. This forms the basis of the application to the JP and **should contain all information that is relied upon**.

e) The original RIPA authorisation or notice should be shown to the JP but will be retained by the Council so that it is available for inspection by the Commissioners' offices and in the event of any legal challenge or investigations by the Investigatory Powers Tribunal (IPT). The court may wish to take a copy.

f) In addition, the Council will provide the JP with a partially completed judicial application/order form

g) Although the Council is required to provide a brief summary of the circumstances of the case on the judicial application form, this is supplementary to and does not replace the need to supply the original RIPA authorisation as well.

h) The order section of the form will be completed by the JP and will be the official record of the JP's decision. The Council will need to obtain judicial approval for all initial RIPA authorisations/applications and renewals and the Council will need to retain a copy of the judicial application/order form after it has been signed by the JP. There is no requirement for the JP to consider either cancellations or internal reviews.

Arranging a Hearing

i) Officers should establish contact with HMCTS administration at the magistrates' court. HMCTS administration will be the first point of contact for the Council when seeking a

j) **Urgent cases.** On the rare occasions where out of hours access to a JP is required then it will be for the Council to make local arrangements with the relevant HMCTS legal staff. In these cases the Council will need to provide two partially completed judicial application/order forms so that one can be retained by the JP. The Council should provide the court with a copy of the signed judicial application/order form the next working day.

k) In most emergency situations where the police have power to act, then they are able to authorise activity under RIPA without prior JP 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).

l) Where renewals are timetabled to fall outside of court hours, for example during a holiday period, it is the Council'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.

Attending a Hearing

m) The hearing is a 'legal proceeding' and therefore Council officers need to be formally designated to appear under its Constitution be sworn in and present evidence or provide information as required by the JP.

n) The hearing will be in private and heard by a single JP who will read and consider the RIPA authorisation or notice and the judicial application/order form. He/she may have questions to clarify points or require additional reassurance on particular matters.

o) The Council will want to consider who is best able to answer the JP's questions on the policy and practice of conducting covert operations and detail of the case itself. It is envisaged that the case investigator will be able to fulfil this role. The investigator will know the most about the investigation and will have determined that use of a covert technique is required in order to progress a particular case. This does not, however, remove or reduce in any way the duty of the Authorising Officer to determine whether the tests of necessity and proportionality have been met. Similarly, it does not remove or reduce the need for the forms and supporting papers that the Authorising Officer has considered and which are provided to the JP to make the case.

p) It is not envisaged that the skills of legally trained personnel will be required to make the case to the JP and this would be likely to, unnecessarily, increase the costs of Council applications.

q) **Officers who are not solicitors** can appear in the Magistrates' on behalf of the Council under section 223 of the Local Government Act 1972, so long as they have been properly authorised to do so in accordance with the Council's Constitution. Such officers should take to court a copy of any such authorisation in case it is asked for by a JP or the Court Clerk.

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

Local authority investigator wants to use a RIPA technique (directed surveillance, CHIS (covert human intelligence source) or communications data).

Does investigator intend to use Directed surveillance?

Is the local authority investigating an offence and does that offence attract a maximum custodial sentence of 6 month or more?

Is the offence being investigated either:
-Section 146/147/147A of the Licensing Act 2003, or
.Section 7 of the Children and Young Persons Act 1993.

• Complete RIPA authorisation/ Notice form, and seek approval of authorising officer/designated person as per current arrangements
• Complete application part of the judicial application/order form for JP.

Within Office Hours
Local authority investigator to contact Her Majesty's Courts & Tribunals Service (HMCTS) administration at the magistrates' court to arrange a hearing.

Attend court with:
• counter-signed RIPA authorisation/ or notice (for CD authorisations/ notices the signatures may be electronic signatures).
• the accompanying judicial application/order form.
• any other relevant reference or supporting material.

Outcome

Outside usual office hours:

A JP may consider an authorisation out of hours in exceptional circumstances. If the authorisation is urgent and cannot be handled the next working day then you should:
• Phone the court's out of hours HMCTS legal staff contact. You will be asked about the basic facts and urgency of the authorisation. If the police are involved in the investigation you will need to address why they cannot make a RIPA authorisation.
• If urgency is agreed, then arrangements will be made for a suitable JP to consider the application. You will be told where to attend and give evidence.
• Attend hearing as directed with two copies of both the counter-signed RIPA authorisation form or notice and the accompanying judicial application/order form.

Investigator may not use directed surveillance. The case should be investigated by other means. Continue to assess if threshold is met if further offences come to light as the case progresses.

Refuse to approve the grant or renewal and quash the authorisation or notice.

Refuse to approve the grant or renewal of an authorisation or notice.

Approve the grant or renewal of an authorisation or notice.

This may be appropriate if the JP considers that an application is fundamentally flawed. The local authority must be given at least 2 business days in which to make representations before the authorisation is quashed. In these circumstances a local authority cannot use the technique and will need to seek fresh authorisation internally before reapplying.

The grant or renewal of the RIPA authorisation or notice will not take effect and the local authority may not use the covert technique. Local authority may wish to address, for example, a technical error and reapply.

Technique may be used in this case. Investigator to resubmit to the JP any renewal or authorisation for the use of a different technique in this case.

Obtain signed order and retain original RIPA authorisation/notice.
For CD authorisations or notices, local authority investigator to provide additional copy of judicial order to the SPoC.
If out of hours, a copy of the signed order to be provided to the court the next working day.

APPENDIX 4

Up to date RIPA forms are available at

https://www.gov.uk/government/collections/ripa-forms--2

APPENDIX 5

NAFN Designated Officers

Title of Officer	Service Area
Head of Consumer Protection & Business Compliance	Neighbourhood Services Private Rented Housing Housing
Head of Neighbourhood Services	Trading Standards Licensing Food Safety Health & Safety