DARTFORD BOROUGH COUNCIL

POLICY STATEMENT

Regulation of Investigatory Powers Act 2000 (RIPA) (as amended)

Adopted by Cabinet 22 April 2010 [Min.No.179]
Reviewed and adopted by Cabinet 25 October 2012 [Min.No.85]
Reviewed and amended under the Managing Director's delegated authority September 2015
Reviewed and amended under the Managing Director's delegated authority October 2018
Reviewed and amended under the Managing Director's delegated authority January 2019
Reviewed and amended under the Managing Director's delegated authority August 2019
Reviewed and amended under the Strategic Director's delegated authority- 16 June 2020
Reviewed and amended under the Chief Officer & Director of Corporate Services delegated authority- 20 August 2022
Reviewed and amended under the Chief Officer & Director of Corporate Services delegated authority- 13 January 2023
Reviewed and amended under the Monitoring Officer's delegated authority- 6 March 2023

INDEX

PART 1

PART 2

PART 3

PART 4

PART 5

PART 6

PART 1

1. Introduction

The Regulation of Investigatory Powers Act 2000 (as amended) (RIPA) and the regulations and orders made thereunder provide the legislative framework within which covert surveillance operations (directed surveillance, deployment of a covert human intelligence source and access to communications data) must be conducted in order to ensure that investigatory powers are used in accordance with human rights. This Policy Statement is intended as a practical reference guide for Council Officers/investigators who may be involved in covert operations.

Officers involved in covert operations, must familiarise themselves with the IPCO's[1] Procedures & Guidance[2], the Code of Practice on Covert Surveillance and Property Interference[3], the Code of Practice on Covert Human Intelligence Sources[4], the Code of Practice on Acquisition and Disclosure of Communications Data[5], and Home Office guidance on the judicial approval process for RIPA and the crime threshold for directed surveillance[6], in order to ensure that they fully understand their responsibilities (the Home Office Codes as updated from time to time).

The right to respect for one's private and family life is enshrined in Article 8 of the European Convention on Human Rights (Convention) which renders it unlawful for a public authority to act in a way, which is incompatible with any of the Convention rights. As with many of the rights in the Convention, the right to privacy is not an absolute right and is subject to certain exemptions.

RIPA and regulations provide an exemption from the right to privacy in certain circumstances, and allow public bodies to interfere with the individual's right to privacy in circumstances that amount to covert surveillance.

The Council is committed to implementing the provisions of RIPA to ensure that any covert surveillance carried out during the course of investigations is undertaken properly and that the surveillance is necessary and proportionate to the alleged offence/s. The Council seeks to ensure that this Policy Statement remains consistent with the Council's objectives.

This Policy Statement ensures:

- that proper procedures are in place in order to carry out covert surveillance;
- that an individual's right to privacy is not breached without justification;
- that the potential invasion of privacy caused by using techniques regulated by RIPA, are properly justified in a clear, concise paper/electronic trail;
- that proper authorisation is obtained for covert surveillance;
- that covert surveillance is considered as a last resort, having exhausted all other avenues;
- that the seriousness of the offence is considered, in addition to the requirement to weigh up the benefits to the investigation, when considering whether to authorise covert techniques under RIPA;
- that the approval of a Magistrate is obtained before the use of a covert technique;
- that an officer is designated as the Single Responsible Officer (SRO) for ensuring that all authorising officers meet the standards required by IPCO;
- that Cabinet has a strategic oversight role in/of the Council's RIPA process.

[1] Investigatory Power Commissioner's Office
[2] Issued April 2021
[3] April 2018 revised December 2022 -The Council has no power to undertake intrusive surveillance operations or enter or interfere with property or wireless telegraphy
[4] December 2022
[5] Issued September 2010 and updated May 2015
[6] Issued October 2012 and revised December 2014

2. External oversight of the Council's RIPA processes – Investigatory Powers Commissioner's Office

The Investigatory Powers Commissioner's Office (IPCO) aims to provide effective and efficient oversight of the conduct of directed surveillance and covert human intelligence sources by public authorities. The Council is usually inspected by IPCO, every three years – the last inspection took place in January 2019.

---

3. Senior Responsible Officer (SRO) and Single Point of Contact (SPOC)

(Covert Surveillance and Property Interference Code of Practice and Covert Human Intelligence Sources Code of Practice and Code of Practice on Acquisition and Disclosure of Communications Data)

The Head of Legal Services and Monitoring Officer is designated the Council's SRO with responsibilities for:

(a) ensuring the integrity of the Council's RIPA processes;
(b) ensuring compliance with RIPA legislation and the Home Office Codes of Practice;
(c) engaging with the IPCO when its inspector conducts an inspection;
(d) overseeing the implementation of any post - inspection plans;
(e) ensuring that all Authorising Officers are of an appropriate standard in light of any recommendations made by the IPCO inspection reports;
(f) ensuring that concerns are addressed, where IPCO inspection reports highlight concerns about the standards of Authorising Officers;
(g) ensuring that the Monitoring Officer's annual report to the Audit Board updates Members on the Council's use (if any) of the RIPA powers.

In the case of communications data, the RIPA authorisation or Section 22 Notice will be scrutinised by a single point of contact (a 'SPOC'). The Council has a membership agreement with NAFN. As a member of NAFN, it is open to the Council to take up their RIPA SPOC service.

---

4. Authorising Officers and Designated Persons

(Covert Surveillance and Property Interference Code of Practice) and Covert Human Intelligence Sources Code of Practice and Code of Practice on Acquisition and Disclosure of Communications Data)

'Director, Head of Service, Service Manager or equivalent' are the terms used for the appropriate level of authorisation within local authorities in the statutory instrument that prescribes the offices, ranks and positions for authorisation purposes (The Regulation of Investigatory Powers (Directed Surveillance and Covert Human Intelligence Sources) Order 2010). The Council interprets the level of authorisation as follows:

- All Directors are Authorising Officers who may also act in urgent cases. These posts are also Designated Persons for the purposes of access to communications data.
- Where there is a likelihood that legally privileged, personal confidential information, confidential constituent information between the MP and a constituent or confidential journalistic material will be acquired as a result of a directed surveillance operation, authorisation will be by the Chief Officer and Director of Corporate Services or in their absence, the Director of Housing and Public Protection or the Director of Growth and Community.
- Authorising Officers cannot delegate their function to an Officer who is not authorised by the 2010 Order, but 'upwards' delegation is possible.

---

5. Cabinet responsibilities

(Covert Surveillance and Property Interference Code of Practice and Covert Human Intelligence Sources Code of Practice)

RIPA is a Cabinet function within the meaning of the Local Authorities (Functions and Responsibilities) (England) Regulations 2000 (as amended).

The review of this Policy Statement, to ensure fitness for purpose, has been delegated by Cabinet to the Head of Legal Services, as the Senior Responsible Officer with responsibilities

for ensuring the integrity of the Council's RIPA processes. The review provides an additional safeguard against inappropriate or disproportionate use of the RIPA powers.

Unless there have been nil returns to IPCO, Cabinet will receive reports on the use of RIPA, to ensure that RIPA is being used consistently and in accordance with this Policy Statement. Reports are presented in such a way that individuals and/or organisations that have been/are the subject of an authorisation, are not identifiable.

Cabinet is not involved in making decisions on specific authorisations.

---

6. Meaning of covert surveillance

(Covert Surveillance and Property Interference Code of Practice)

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

Surveillance includes monitoring, observing or listening to persons, their movements, their conversations, or other activities or communication.

RIPA provides for the authorisation of covert surveillance where that surveillance is likely to result in the obtaining of *private information* about a person.

Investigating Officers need to 'freeze frame' their thoughts just before the moment of surveillance and interrogate their intentions:

- are they trying to be hidden? or
- are they not bothered? or
- do they want the person who is the subject of the investigation to be aware of them?

It may mean Investigating Officers choosing whether to be preventative or enforcement focussed in a particular situation.

REMEMBER: if you are trying to be overt, can you prove this if challenged in Court? Analyse your thought processes and intentions to give you the answers. If your activities are not hidden from the subjects you are investigating, RIPA does not apply.

The Council does not have the power to interfere with property or wireless telegraphy or undertake intrusive surveillance operations (i.e. covert surveillance in relation to anything taking place on residential premises or a private vehicle carried out either by a person or device inside residential premises or a private vehicle or by a device placed outside).

---

7. Meaning of private information

(Covert Surveillance and Property Interference Code of Practice)

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

Private information includes any information relating to a person's private or family life and is taken generally to include any aspect of a person's private or personal relationship with others, including family and professional or business relationships.
Whilst a person may have a reduced expectation of privacy when in a public place, covert surveillance of that person's activities in public, may still result in the obtaining of private

information e.g. CCTV footage of a person attempting suicide released to the media showing the person's photo – the Court held that the people viewing the CCTV footage exceeded to a far greater degree any exposure that would have been caused by an ordinary passer-by and as the person's identity had not been adequately masked in the publicised footage, there was a serious interference with his private life – the insufficiency of safeguards when compared with the interference with the person's private life was disproportionate.

A drone can be a very useful tool to use in an investigation.

Use of a drone has the potential to capture private information. Collateral intrusion is also highly likely when using a drone.

If there is the potential to gather personal information, the subject of the investigation and/or the landowner will either need to be notified of the use of the drone (such that any use of the drone is not covert), or a RIPA authorisation will be needed.

If the drone is to be flown over a residential area or highly populated area, where the potential for collateral intrusion is high, notification that the drone will be used, will be published on the Council's website prior to the flight.

Obtaining private information is likely to be the case where a person has a reasonable expectation of privacy even though acting in public e.g. during leisure hours or activities.

As a general rule of thumb, there is a great risk of likelihood of obtaining private information if doing observations around a person's home. The risk is lessened, but still there, if observing people in public, but during leisure hours or activities. The risk may lessen but still be there around solely commercial premises observed during business hours, as the firm's employees are made up of private individuals and also by the liberal interpretation by the Courts, of Article 8.

Base your decision on your knowledge of the site on a case-by-case basis to determine if you need a RIPA authorisation.

Where covert surveillance activities are unlikely to result in the obtaining of private information about a person, or where there is a separate legal basis for such activities, neither RIPA nor the Codes of Practice need apply.

8. Meaning of directed surveillance

(Covert Surveillance and Property Interference Code of Practice)

Directed surveillance is defined in RIPA as surveillance that is covert but not intrusive and is conducted:

- for the purposes of a specific operation or investigation;
- in such a manner that it is likely to result in the obtaining of private information about a person (whether or not they are the individual specifically identified for the purposes of the investigation or operation);
- 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 carrying out surveillance.

9. For what purposes can the Council conduct directed surveillance?

(see Article 7A of the Regulation of Investigatory Powers (Directed Surveillance and Covert Human Intelligence Sources) Order 2010 (as amended) and section 55 of the Home Office guidance on the judicial approval process for RIPA and the crime threshold for directed surveillance)

The Council can use directed surveillance only for the purpose of preventing and detecting conduct, which constitutes one or more criminal offences and it meets one of the following conditions:

(a) that the criminal offence which is sought to be prevented or detected is punishable, whether on summary conviction or on indictment, by a maximum term of at least 6 months of imprisonment; or

(b) would constitute an offence under sections 146, 147 or 147A of the Licensing Act 2003 or section 7 of the Children and Young Persons Act 1933 (all offences involving sale of tobacco and alcohol to underage children).

Examples of offences, which meet the serious crime, test (para. (a) above) include:

- Benefit Fraud (Section 111A of the Social Security Administration Act 1992 and the Fraud Act 2006;
- Fly tipping;
- Some Planning offences (e.g. making false statements to obtain a Certificate of Lawful Development).

Investigating Officers must always check the applicable legislation to ensure that any proposed directed surveillance complies with the serious crime test.

The following offences are not covered by the serious crime test:

- Littering;
- Dog fouling;
- Fly posting;
- Most planning offences involving stop notices, enforcement notices, untidy site notices, planning contravention notices, breach of condition notices and tree preservation orders.

The Council will need to seek judicial approval of the grant or renewal of a directed surveillance authorisation (refer to Part 5 of this Policy Statement)

10. Activities/operations involving directed surveillance

(see Chapter 2 Covert Surveillance and Property Interference Code of Practice)

Subject to the serious crime test in section 9 of this Policy Statement, it is safest to assume that any operation that involves planned covert surveillance of a specific person or persons (including Council employees) likely to obtain private information, of however short a duration, falls within the definition of directed surveillance and will, therefore, be subject to authorisation under RIPA.

The consequence of not obtaining an authorisation and the approval of a Magistrate for a covert surveillance operation will render the surveillance action unlawful under the Convention, or any evidence obtained may be inadmissible in Court proceedings. Council Officers must seek an authorisation and a Magistrate's approval, where the surveillance is likely to interfere with a person's Article 8 rights to privacy. Obtaining an authorisation and a Magistrate's approval will ensure that the surveillance action is carried out in accordance with the law and is subject to stringent safeguards against abuse.

Proper authorisation and judicial approval of a covert surveillance operation should also ensure the admissibility of evidence under the common law, PACE (Section 78) and the Convention. Covert surveillance operations must at all times be justified and proportionate and necessary (JAPAN).

The Home Office Code of Practice on Covert Surveillance and Property Interference (see section 3.39) refers to the covert use of overt CCTV and ANPR systems, e.g. where a Council Officer with regulatory responsibilities requests Town Centre Management CCTV operators to track a particular individual who has been identified in the Town Centre undertaking illegal trading or licensing activities. The Code clearly indicates that such targeted directed surveillance activity, should be subject to RIPA authorisation.

Subject to the serious crime test in section 9 of this Policy Statement, directed surveillance might be used, for example:

(a) in fraud cases where there is a need to observe a person's home in order to find out who the landlord is, or to find out who the resident has associations with;
(b) by placing a stationary mobile or video camera outside a building to record antisocial behaviour on residential estates.
(c) CCTV cameras targeting a particular known offender at the request of the Police in tracking the perpetrator's activities, as part of a pre-planned investigation (NB: if an operation has a number of different potential targets and for the purposes of a specific investigation or specific operation, it can fall within RIPA.
(d) a person being observed by Environmental Health for running a commercial business of cake making from her home – although the investigation relates to the business, any surveillance is likely to result in the obtaining of private information.
(f) 'drive by' past a café to establish a pattern of occupancy of the premises by any person – as the accumulation of evidence is likely to result in the containing of private information about that person.
(g) the use of professional witnesses by the Council to obtain information about an individual.

11. Activities/operations not involving directed surveillance

(Covert Surveillance and Property Interference Code of Practice)

Directed surveillance is conducted where it involves the observation of a person or persons with the intention of gathering private information to produce a detailed picture of a person's life, activities and associations. Private information includes any information relating to the person's private or family life. However, it does not include general observation that is part of an Enforcement Officer's normal work.

General observation duties of the Council's Enforcement Officers whether overt or covert, frequently form part of their day to day activities and the Council's legislative core functions – such activities will not normally require a directed surveillance authorisation and judicial approval. Remember to complete the 'Application for authorisation to conduct an OVERT investigation ' (on the intranet).

Examples

(a) Enforcement Officer attendance at a car boot sale where it is suspected that counterfeit goods are being sold. In such a case, the Officer is not carrying out surveillance of particular individuals - the intention is, through reactive enforcement, to identify and tackle offenders. The obtaining of private information is unlikely.
(b) Observing a construction site prior to a visit, or videoing scaffold erectors prior to a visit for the purpose of identifying problems, or stopping on a hill and using binoculars to identify where potential unlawful activities are taking place, do not constitute directed surveillance. Similarly, watching premises where it is alleged that alcohol is being sold to children, or making a test purchase, do not constitute directed surveillance.
(c) The covert recording (with a DAT recorder) by Environmental Health Officers of suspected noise nuisance, where the intention is only to record excessive noise levels from adjoining premises and the recording device is calibrated to record only excessive noise levels, and the offender is warned* that if the level of noise continues, recording will occur. In such circumstances, the offender will normally be regarded as forfeiting any claim to privacy.
(d) The recording, whether covert or overt, by an Enforcement Officer, of an interview with a member of the public, where it is made clear by the Enforcement Officer that he is a Council employee and that the interview is voluntary. In such circumstances, the person being interviewed knows that the interview is being conducted by a Council Officer and that the information will pass into the Council's possession.
(e) Anything, which constitutes an immediate response e.g. a Council Officer with regulatory responsibilities, may by chance be present when an individual is potentially infringing the

law and it is necessary to observe, follow, or engage in other surveillance tactics as an instant response to the situation to gather further information or evidence. Once this immediacy has passed, however, any further directed surveillance of the individual, must be subject to RIPA authorisation.

(f) Warning* letters issued to householders about spot checks of their bins and openly carrying out the checks.

(g) Sufficient detailed warning letters to alleged perpetrators of the types and timescale of surveillance that may be taken by the Council e.g. Environmental Health leaflets describing surveillance over a three month period by officers/and/or the use of DAT recorders or matron boxes.

(h) Where the Council relies on statutory powers such as powers of entry – this negates the need for a RIPA even where the investigation may fit the RIPA criteria.

(i) Investigating staff for employment matters.

(j) Overt CCTV will not normally require a RIPA as members of the public are aware these are in place and because their operation is covered by the Data Protection Act 2018, UK GDPR[7], the Surveillance Camera Code of Practice and the Information Commissioner's guidance on CCTV.

(k) Automatic Number Plate Recognition (ANPR) cameras used to monitor traffic flow.

(l) In anti-social behaviour litigation or enforcement cases, where Council Officers ask residents to maintain diary notes of anti-social behaviour incidences or planning control breaches (but see section 14 below).

(m) 'Keeping a general eye out' - but note if it is more like 'every Thursday between the hours of 2 and 3a.m. for the next 6 weeks, target cameras in xx spot for 2 people in a white car who throw out old fridges and freezers' is more specific and likely to need a RIPA.

(n) 'Drive by' past a café for the purpose of obtaining a photograph of the exterior.

*Warning letters etc. are valid only for 3 months.

Please note that if you have time to think about it, plan it and undertake targeted surveillance on a specific person or persons, you also have the time to consider RIPA requirements and use them when appropriate.

Remember: **IF IN DOUBT GET IT AUTHORISED AND OBTAIN JUDICIAL APPROVAL.**

12. Covert human intelligence source (CHIS)

(Covert Human Intelligence Sources Code of Practice)

The Council can use CHIS where it is necessary for the purpose of preventing or detecting crime or of preventing disorder.

The Council will need to seek judicial approval of the grant or renewal of a CHIS authorisation (refer to Part 5 of this Policy Statement)

The use of 'undercover officers' or 'informants' in a covert manner, can on occasions, be a valuable resource for the protection of the public and the maintenance of law and order. A person is a CHIS if:

- h/she establishes or maintains a personal or other relationship with a person for the covert purpose of facilitating the doing of anything falling within the two bullet points below;
- he/she covertly uses such a relationship to obtain information or to provide access to information to another person; or
- he/she covertly discloses information obtained by the use of such a relationship or as a consequence of the existence of such a relationship.

[7] Derived from the General Data Protection Regulation (EU) 2016/679

Unlike directed surveillance, which relates specifically to private information, authorisations for the use or conduct of a CHIS do not relate specifically to private information, but to the covert manipulation of a relationship to gain any information. By the very nature of the activity/operation, the use of a CHIS may constitute interference with a person's right to privacy under Article 8 of the Convention (the right to respect for private and family life). It is therefore strongly recommended that the Council considers an authorisation for the use or conduct of a CHIS, whether for the purposes of obtaining information, particularly private information, or simply through the covert manipulation of a relationship.

CHIS will be more commonly used by the Police, HM Revenue & Customs, and intelligence/security services where it is normal practice to use agents, informants and officers working undercover.

It is important to recognise that in some rare situations, directed surveillance and CHIS may both apply. The use of a CHIS by the Council, is however, likely to be relatively infrequent.

Remember, **IF IN DOUBT, GET IT AUTHORISED AND OBTAIN JUDICIAL APPROVAL.**

13. Activities/operations involving CHIS

There are occasions, however, when the Council may use a CHIS to obtain information e.g.

- a CHIS may be used as a source to obtain information in respect of an investigation into Housing or Council Tax Benefit fraud; this may be a Council Officer acting undercover.
- a CHIS may be used as a source to obtain information in respect of an investigation into the loss of monies at Council premises where there are cashier activities; this may be a Council Officer acting undercover.
- a professional witness CHIS posing as a neighbour to obtain evidence.

This list is clearly not definitive. There is an element of judgement involved in determining when an individual taking some part in an investigation may be acting as a CHIS and the matter is not entirely black and white; if in doubt take advice from Legal Services.

Please refer to Part 3 of this Policy Statement for guidance on 'test purchases'.

14. Activities/operations not involving CHIS

The following situations will not normally require a relationship to be established for the covert purpose of obtaining information:

- test purchase transactions carried out in the normal course of business, where Officers do not establish a personal or other relationship e.g. the purchase of a music CD for subsequent expert examination would not require authorisation, but where the intention is to ascertain whether a trader is taking delivery of suspected fakes and a relationship is established between the trader and the Officer, then authorisation should be sought beforehand;
- the task of ascertaining purely factual information e.g. the location of cigarette vending machines in licensed premises;
- where members of the public volunteer information to an Officer as part of their normal duties;
- where the public call telephone numbers set up by the Council to receive information;
- where members of the public are asked to keep diaries of incidents in relation to planning enforcement or anti-social behaviour – however please note that such activity will be regarded as directed surveillance, requiring an authorisation if it is likely to result in the obtaining of private information about a person (whether or not one specifically identified for the purposes of the investigation or operation).

15. Proportionality and necessity

(Covert Surveillance Covert Surveillance and Property Interference Code of Practice and Covert Human Intelligence Sources Code of Practice and Code of Practice on Acquisition and Disclosure of Communications Data)

Proportionality - this is a fundamental principle embodied in the Convention. Officers must be able to demonstrate that a covert surveillance operation justifies the level of intrusion of privacy that may occur with regard to the target or targets of the surveillance or any other persons i.e. that it is proportionate set against the outcome. Authorising Officers must believe that the activities to be authorised, are necessary in relation to:

(a) directed surveillance - for the purpose of preventing and detecting conduct, which constitutes one or more criminal offences and it meets one of the conditions referred to in section 9 of this Policy Statement;
(b) CHIS - for the purpose of preventing and detecting crime or of preventing disorder;
(c) access to communications data - for the purpose of preventing and detecting crime or of preventing disorder;

AND that the activities are proportionate to what is sought to be achieved by carrying them out. This involves balancing the seriousness of the intrusion into the privacy of the target or any other person affected by the covert surveillance, against the need for the activity, in investigative and operational terms.

The reasons why the activity is considered proportionate must be adequately recorded in the application form. It is not enough to simply have a standard phrase saying that the surveillance is proportionate. The rationale for proceeding with covert surveillance needs to be written and explicit. Consider the following in framing responses to questions included in the application form:

- balance the size and scope of the proposed activity against the gravity and extent of the perceived crime or offence;
- explain how and why the methods to be adopted will cause the least possible intrusion on the subject and others;
- consider whether the activity is an appropriate use of the legislation and a reasonable way, having considered all reasonable alternatives, of obtaining the necessary result;
- evidence, as far as reasonably practicable, what other methods have been considered and why they are not being implemented.

Proportionality in this context, has nothing whatsoever to do with whether or not the possible benefits of a covert surveillance operation justifies the time and money expended by the Council, although Officers will no doubt wish to take this into account.

The Authorising Officer will only grant an authority if covert surveillance operations are necessary in the circumstances of the particular case and only for the purpose referred to in para. (a), (b) or (c) above.

The Authorising Officer will give consideration to alternative means of obtaining the information required for a directed surveillance or CHIS e.g. by obtaining statements from witnesses (if available) and will evidence as far as is reasonably practicable, what other methods have been considered and why they were not implemented.

The Authorising Officer/Designated Person will explain how and why the methods to be adopted will cause the least possible intrusion on the target and others.

The Authorising Officer will consider whether the directed surveillance or CHIS activity is an appropriate and reasonable use of the legislation, having considered all reasonable alternatives of obtaining the necessary result.

The authorisation will not be proportionate if it is excessive in the overall circumstances of the case. Each action authorised should bring an expected benefit to the investigation or operation and should not be disproportionate or arbitrary.

16. Collateral intrusion

(Covert Surveillance and Property Interference Code of Practice and Covert Human Intelligence Sources Code of Practice)

The Authorising Officer will take into account the risk of collateral intrusion into the privacy of persons other than those who are the direct subjects of the operational investigation, such as innocent bystanders. Measures will be taken wherever practical, to avoid unnecessary intrusion into the lives of those not directly involved in the operation. For example, an investigator may seek to conduct directed surveillance of T, because T is suspected of housing benefit fraud. The surveillance may unavoidably result in the obtaining of some information about T's family members who are not the intended subjects of the surveillance. The Authorising Officer must consider the proportionality of this collateral intrusion and whether sufficient measures are to be taken to limit it, when granting the authorisation.

All applications for covert surveillance operations must include an assessment of the risk of collateral intrusion and details of any measures taken to limit this, to enable the Authorising Officer/Designated Person fully to consider the proportionality of the proposed actions.

The same proportionality test applies to the likelihood of collateral intrusion, as to intrusion into the privacy of the intended subject of surveillance.

17. Collaborative working

(Covert Surveillance and Property Interference Code of Practice and Covert Human Intelligence Sources Code of Practice)

Officers need to be aware of particular sensitivities in the local community where the directed surveillance or CHIS is likely to take place and of any other similar activities being undertaken by other law enforcement agencies e.g. the Police, which could impact on the deployment of surveillance or CHIS.

Where conflicts might arise, the Authorising Officer must consult with a senior officer within the Police force area in which the investigation is to take place.

Where the operational support of the Police or other agencies is foreseen, this must be specified in the authorisation. Directed surveillance or CHIS as part of a joint operation, only requires one authorisation.

18. Legally privileged information, personal confidential information or confidential journalistic material

(Covert Surveillance and Property Interference Code of Practice Covert Human Intelligence Sources Code of Practice)

'Confidential material' is described by RIPA as being:

(a) matters subject to legal privilege;
(b) confidential constituent information between the MP and a constituent in respect of constituency matters;
(c) confidential personal information; or
(d) confidential journalistic material.

Approval must be granted by the Head of Paid Service and in her absence, by the Monitoring Officer.

A substantial proportion of communications between a lawyer and client may be subject to legal privilege. Matters subject to legal privilege must be kept separate from enforcement investigations or criminal prosecutions, as they will not be admissible in court

Where the activities of a CHIS will result in the CHIS obtaining, providing access to or disclosing matters subject to legal privilege, the authorising officer must obtain the prior

approval of the IPCO before authorising the CHIS. As part of the judicial approval process, copy of any IPCO approval must be provided to the Magistrate.

and written communications are held in confidence if subject to an express or implied undertaking to hold the communications in confidence or where such communications are subject to a restriction on disclosure or an obligation of confidentiality contained in legislation e.g. consultations between a health professional and a patient, information from a patient's records or information relating to the spiritual counselling of a person.

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 an undertaking. The attention of the Commissioner should be drawn to confidential journalistic material during the IPCO inspection and the material made available to the inspector, if requested.

Acquiring material in the manner referred to above, is likely to be rare for the Council.

---

19. Pending or future criminal or civil investigations

(Covert Human Intelligence Sources Code of Practice)

Material obtained under directed surveillance or CHIS authorisations, may be used as evidence in criminal proceedings and to further other investigations.

---

20. Records management

(Covert Surveillance and Property Interference Code of Practice and Covert Human Intelligence Sources Code of Practice)

The Freedom of Information Act 2000 requires public authorities to maintain efficient record management systems in order to comply with requests for information. Retention periods for information held by the Council, are detailed in the Council's Data Retention Policy & Schedule (retention periods are based on legal, common practice, financial and/or administrative requirements).

All material obtained as a result of having undertaken a directed surveillance or CHIS will be recorded and logged in the Investigating Officer's notebook in accordance with usual procedures for logging of evidence.

Confidential material will only be disseminated outside the Council where this has been expressly authorised by the Authorising Officer/Designated Person, having taken the necessary legal advice.

Reasonable steps will be taken to ensure that confidential information is securely stored and cannot fall into the wrong hands.

All confidential information (as defined in Part 1, section 18 of this Policy Statement) will be destroyed as soon as it is no longer necessary to retain it for the specified purpose. Regular review of material obtained as a result of covert surveillance will ensure that material is destroyed when its retention can no longer be justified.

The records kept by the Council will be maintained in such a way as to preserve the confidentiality, or prevent disclosure of the identity of the covert surveillance target, and the information provided by a CHIS.

The Data Protection Officer ensures that data retention & disposal arrangements are in place for the secure handling, storage and destruction of material obtained through the use of covert surveillance operations. The Council's Records Management Policy details the framework for the management of records within the Council. The Chief Officer & Director of Corporate Services) maintains an overview of the Records Management Policy.

Authorising Officers must ensure compliance with the data protection requirements under the Data Protection Act 2018 and UK GDPR and the relevant codes of practice produced by the Council, relating to the handling, storage and destruction of covert surveillance operations and CHIS material.

---

21. Using surveillance equipment

Officers conducting surveillance must endeavour to use any equipment that is necessary in the conduct of such surveillance in a responsible and discrete manner. Officers should be particularly wary that the use of any surveillance equipment is restricted to being used in a manner that constitutes covert surveillance only. In instances where there is a risk that the use of such equipment will transform the operation into an intrusive one, the surveillance should cease.

Upon the cessation of surveillance, Officers should ensure that any equipment is properly checked upon its return to storage, both as to condition and to ensure that it does not contain material that could fall into the possession of unauthorised staff e.g. staff should ensure that any video tapes, discs etc. are removed from the equipment prior to storage and possible use by other persons.

If any faults with the equipment are detected, this should be brought to the attention of the Authorising Officer as soon as possible. Under no circumstances should the Authorising Officer seek to rectify any faults, as this could affect admissibility of the evidence.

---

22. Access to Communications Data (ACD) – Appendix B Flowchart

(Chapter II part I of the Regulation of Investigatory Powers Act 2000 (as amended) and Acquisition and Disclosure of Communications Data Code of Practice)

The Council may obtain postal and telecommunications data for purposes related specifically to and only for the prevention or detection of crime and/or prevention of disorder.

The term communications data embraces ‘who, ‘when’ and ‘where’ of a communication and can include all phone-calls made and received, who the person is in contact with, the geographic location of calls made from mobile phones, emails sent and received, websites visited and television programmes watched.

The most relevant aspects of ‘communication data’ for the Council will be the name and address of the subscriber and registered user of the telephony (mobile and/or land line) or registered user of an IP/email address. It does not however include the actual content of emails or phone conversations etc.

In the case of a letter sent in the post, that data might include the names of the addressee and sender and a post mark showing where and when it was posted, all of which are on the outside of the envelope. It would not include the contents of the letter itself. Similarly, with calls from a mobile phone, communications data can comprise the telephone numbers involved, and the time and place of the call, but not what was said.

Whilst access to this information will not involve intercepting or tracking a communication, it can still involve a substantial interference with a person’s right to privacy. The strict tests of “necessity” and “proportionality” referred to in section 15 of this Policy Statement must therefore be met before any communications data is obtained. Collateral intrusion (i.e. impact on third parties) must be avoided or minimised as much as possible (see section 16 of this Policy Statement).

The Council will need to seek judicial approval of the grant or renewal of an access to communication data authorisation or of the giving or renewal of a Section 22 Notice (refer to Part 5 of this Policy Statement)

---

23. Judicial Approval

The Council must obtain the approval of a Magistrate (Justice of the Peace) for the use of any one of the three covert investigatory techniques available to it under RIPA - namely directed surveillance, the deployment of a CHIS and accessing communications data (ACD).

Please refer to Part 5 and the Flowcharts at Appendices A and B of this Policy Statement, for guidance on the judicial approval process.

24. Training

The IPCO has emphasised the importance of training in RIPA legislation not least because the views on the legislation can be clouded by inexperience and misconceptions. Lack of training may result in Council Officers having difficulty defending their credentials, if challenged.

All investigators and Authorising Officers/Designated Persons are trained on the provisions of RIPA to ensure that the requirements of the law are complied with. Regular update training is provided, to ensure that all personnel involved with the operation of RIPA, are aware of its requirements.

25. Social Networking & Internet Sites

'Repeat viewing of individual 'open source' sites for the purpose of intelligence gathering and data collation should be considered within the context of the protection that RIPA affords to such activity'[8]

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 social networking site 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.

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 e.g. if someone is being monitored through, for example, their Facebook profile for a period of time and a record of the information is kept for later analysis, this is likely to require a RIPA authorisation for directed surveillance (see section 2 of this Policy Statement).

If it is necessary and proportionate for the Council 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 Council Officer or by a person acting on the Council's behalf (i.e. the activity is more than mere reading of the site's content) (see section 2 of this Policy Statement).

[8] OSC Annual RIPA Report (2014)

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.

To avoid the potential for inadvertent or inappropriate use of social network sites in investigative and enforcement roles, Council Officers should be mindful of the following:

- do not create a false identity in order to 'befriend' individuals on social networks without authorisation under RIPA;
- when viewing an individual's public profile on a social network, do so only to the minimum degree necessary and proportionate in order to obtain evidence to support or refute an investigation;
- repeated viewing of open profiles on social networks to gather evidence or to monitor an individual's status, must only take place under a RIPA authorisation;
- 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.

Refer to the Policy for Interrogating Social Media for Investigative Purposes (on the Intranet).

PART 2
AUTHORISATIONS PROCEDURE FOR DIRECTED SURVEILLANCE AND CHIS

1. What is authorisation?

(see Chapter 3 of the Home Office Covert Surveillance and Property Interference Code of Practice and Chapters 3- 5 Covert Human Intelligence Sources Code of Practice)

Authorisation is the process by which a directed surveillance operation or CHIS is subject to proper consideration, recording and approval by the Officer conducting the investigation and the Director authorised to approve it.

An authorisation ensures that all relevant factors have been thoroughly considered and checked. It is also the means by which, in the event of challenge, Officers can demonstrate that directed surveillance or the use of CHIS was lawfully conducted and that it was a fair and reasonable way to proceed, despite the possible intrusion of a person or persons' privacy.

As soon as a plan of action is decided upon which involves directed surveillance or the use of CHIS, the appropriate authorisations should be sought. This involves an Investigating Officer completing the relevant authorisation form at Appendix A.

In general, authorisations should be sought prudently and in advance of the activity constituting the directed surveillance or use of CHIS. The Council is not permitted to orally authorise the use of RIPA techniques. Out of hours arrangements should be in place with the Magistrates' Court to deal with out of hours applications (see Appendix B).

The standard authorisation forms issued by the Home Office and adapted for Council use (Appendix A), cover all of the necessary aspects. It is important that these forms are correctly and adequately completed for all directed surveillance and CHIS operations.

Proportionality, necessity and collateral intrusion are elements of the written application that are of particular importance and an integral part of a number of the questions contained in the standard application forms.

REMEMBER – AUTHORISATIONS WILL NOT TAKE EFFECT UNTIL JUDICIAL APPROVAL HAS BEEN SOUGHT AND GRANTED (see Flowcharts at Appendix B).

2. Authorisation procedure

Must be authorised by the relevant Director as 'Authorising Officer' and requires the personal authority of the Authorising Officer.

1. The Authorising Officer should first satisfy themselves that:
   (a) the directed surveillance authorisation is necessary for the purpose of preventing and detecting conduct, which constitutes one or more criminal offences and it meets one of the conditions referred to in section 9 of this Policy Statement;
   (b) The CHIS authorisation is necessary for the purpose of preventing or detecting crime or of preventing disorder.
2. The Authorising Officer should satisfy themselves that the directed surveillance or CHIS is proportionate to what it seeks to achieve. In many instances, evidence may be obtainable by other routes, other than directed surveillance, e.g. witness statements, official records, the DVLA, etc.
3. The Authorising Officer should consider whether there could be any collateral intrusion on, or interference with, the privacy of person(s), other than the subject of the surveillance. This is particularly relevant where the premises being observed are used by other persons. This must be taken into account by the Authorising Officer when considering whether the need for the surveillance is proportionate to the problem.

4. As a matter of policy, no directed surveillance should be carried out by Council staff that may intrude upon circumstances covered by the Seal of the Confession, which refers to the spiritual counselling between a Minister and a member of their faith.
5. Use the relevant form at Appendix A for an authorisation for directed surveillance or use of CHIS. The form should be completed by the Officer wishing to carry out the directed surveillance or CHIS operation and the Authorising Officer, before any directed surveillance or CHIS operation takes place.
6. Directed surveillance and CHIS might be employed by other agencies with which the Council carries out joint investigations, for example the Police or the Environment Agency. In those instances, care should be taken to determine whether there will be directed surveillance, who by, and who will be authorising its use. It is normally for the tasking agency to obtain or provide the authorisation. If the Council decides that directed surveillance or CHIS is necessary, then it should inform those in the other agencies involved in the joint investigation.
7. The Authorising Officer should not normally be responsible for authorising operations in which they have been directly involved, although this may on occasion, be unavoidable. Where an Authorising Officer authorises such an investigation or operation, the Departmental file and central database should highlight this and the attention of the inspector should be invited to it during the IPCO inspection.
8. The Authorising Officer must be satisfied that the appropriate arrangements are in place for the management of the CHIS[9] including ensuring that the role and responsibilities of the handler and controller are understood and that a risk assessment for health and safety is undertaken).
9. Judicial approval is required before any authorisation for directed surveillance or CHIS can take effect – see the application form at Appendix B and Part 5 to this Policy Statement.
10. The authorisation for directed surveillance or CHIS and any associated papers (other than confidential information as defined in Part 1, section 18 of this Policy Statement), must be retained on the Departmental file and on the central data base for a period of 3 years from the ending of each authorisation, in accordance with the Data Retention Schedule.
11. Confidential information (as defined in Part 1, section 18 of this Policy Statement) will be destroyed as soon as it is no longer necessary to retain it for the specified purpose.
12. The SRO will on request, make the authorisations available for inspection, by the IPCO and to the Investigatory Powers Tribunal.
13. Authorising Officers must ensure compliance with the Data Protection Act 2018 principles and UK GDPR. Your purpose must be legitimate under the data protection legislation. This means it must be reasonable, lawful and appropriate. If you use surveillance for one purpose, you cannot later use the information you collect for a completely different one. Check whether the way you plan to use surveillance gives you a 'lawful basis' for processing data under the UK GDPR. If you are likely to collect sensitive (i.e. 'special category') data – this means you will need to meet extra conditions under the UK GDPR – see the Community Safety including CCTV, Body Worn Cameras, Dash Cams and Environmental Crime - Privacy Notice. Ensure you carry out a Data Protection Impact Assessment (DPIA) and refer to the lawful bases and legal gateways in your DPIA.

3. What is the duration of authorisations?

(Covert Surveillance Covert Surveillance and Property Interference Code of Practice and Covert Human Intelligence Sources Code of Practice)

Once judicially approved in accordance with Part 5 of this Policy Statement, authorisations for a directed surveillance operation will, (unless renewed or cancelled), cease to have effect at the end of a period of three months beginning with the day on which the authorisation took effect e.g. authorised on 20 December 2011: expires 19 March 2012.

[9]Where the Council is working in partnership with the Police, CHIS will be undertaken by the Police. Only in very exceptional circumstances will the Council undertake a CHIS. Please seek legal advice before embarking on a CHIS.

Authorisations for CHIS will, (unless renewed or cancelled) cease to have effect at the end of a period of twelve months beginning with the day on which the authorisation took effect e.g. authorised on 20 December 2011: expires 19 December 2011.

Once judicially approved in accordance with Part 5 of this Policy Statement, written authorisations for a directed surveillance or CHIS operation granted by a Director (as the person entitled to act in urgent cases), will cease to have effect (unless renewed) after seventy-two hours beginning with the time the authorisation was granted or renewed.

4. How is an operation reviewed, renewed or cancelled?

(Covert Surveillance Covert Surveillance and Property Interference Code of Practice and Covert Human Intelligence Sources Code of Practice)

All directed surveillance and CHIS must be effectively assessed and regularly monitored by the Officer conducting the operation and the Authorising Officer. The authorisation process should be viewed as a useful management tool to help Officers to achieve this. Regular reviews of authorisations should be undertaken to assess the need for surveillance to continue. Responsibility for assessing the appropriate review period rests with the Authorising Officer and this should be as frequently as considered necessary and practicable. There is clear guidance on reviews, renewals and cancellations in the Home Office Codes of Practice and Officers should refer to the appropriate sections for further details.

The standard renewal and cancellation forms issued by the Home Office adapted for Council use (Appendix A), cover all the necessary aspects. It is important that these forms are correctly and adequately completed. It is particularly important at the review stage that renewal or cancellation of an operation is considered.

The Authorising Officer who granted or last renewed an authorisation must **cancel** it, if he/she are satisfied that the directed surveillance or CHIS no longer meets the criteria upon which it was originally authorised (see below for more details on the rules relating to cancellations).

Reviews

Regular **reviews** will take place once authorisation has been granted. Except in exceptional circumstances, the review will take place 14 days after a written authorisation has been granted and 24 hours after an urgent authorisation has been granted. Records of reviews will be maintained in the Departmental file and on the central database. Records will be retained in both locations for a period of 3 years, from the ending of each authorisation.

Renewals/Extensions

It will be rare that **renewals/extensions** of authorisations will be required in order to continue surveillance. However, if they are required, applications for renewals of authorisation will be made in writing using a standard renewal proforma (Appendix A).

If the Authorising Officer considers it necessary for the authorisation to continue, then, subject to judicial approval in accordance with Part 5 of this Policy Statement, the authorisation may be renewed/extended as follows:

- for an ordinary authorisation, renewed for a period of up to three months;
- all applications for renewals/extensions will contain the following information:

  - renewal/extension numbers and dates of any previous renewals;
  - details of any significant changes to the information as listed in the original authorisation as it applies at the time of the renewal/extension;
  - the reasons why it is necessary to continue with the directed surveillance or CHIS operation;
  - the reasons why the directed surveillance or CHIS operation is still necessary and proportionate to what it seeks to achieve;
  - the content and value to the investigation or operation of the information so far obtained by the directed surveillance or CHIS operation;
  - details of the results of the regular reviews of the investigation or operation;
  - judicial approval granted by the Magistrate.

Permission to renew/extend directed surveillance or a CHIS operation, will be granted by the Authorising Officer on an exceptional basis. No proforma is provided for renewing/extending approvals. The circumstances will be so unique, that it must be argued on a case-by-case basis.

Records of renewals will be maintained in the Departmental file and on the central database. Records will be retained in both locations for a period of 3 years, from the ending of each authorisation.

Cancellations

Authority to carry out covert surveillance is valid for a period of 3 months, from the date it was granted. However, there is a duty incumbent upon both the Authorising Officer and the Officer carrying out the surveillance, to continually review its necessity and proportionality. The operation must be **cancelled** as soon as it is no longer appropriate, irrespective of the time outstanding. The cancellation must be recorded in writing on the appropriate authorisation form (Appendix A) and retained in the Departmental file and on the central database for 3 years from the ending of each authorisation.

As soon as the decision is made to cancel the authorisation, the directed surveillance or CHIS operation must immediately cease.

---

5. Security and welfare of the CHIS

(Covert Human Intelligence Sources Code of Practice)

There are rules about the use of vulnerable adults or juveniles as sources and there are special requirements with regard to the management, security and welfare of sources. Refer to the Covert Human Intelligence Sources Code of Practice for detailed guidance. In summary:

(a) when deploying a source, the Council should take into account the safety and welfare of that source, when carrying out actions in relation to an authorisation or tasking, including the foreseeable consequences to others, of that tasking.
(b) before authorising the use or conduct of a CHIS, the Authorising Officer should ensure that a risk assessment is carried out to determine the risk to the source of any tasking and the likely consequences, should the role of the source become known. The ongoing security and welfare of the source, after the cancellation of the authorisation, should also be considered at the outset.
(c) the person responsible for the day-to-day management of the source's welfare and security e.g. departmental manager, will bring to the attention of the Authorising Officer, any concerns about the personal circumstances of the source, insofar as they might affect:

- the validity of the risk assessment;
- the conduct of the source, and
- the safety and welfare of the source.

Where deemed appropriate, the concerns about such matters should be considered by the Authorising Officer and a decision taken on whether or not to allow the authorisation to continue.

PART 3

TEST PURCHASES

In some instances, the tasking given to a person will not require the source to establish a personal or other relationship for a covert purpose e.g. an Environmental Health Officer may be involved in the test purchase of items that are unfit for consumption. In such cases, it is for the Council to determine where, and in what circumstances, such activity may require authorisation.

It is the view of the Home Office that, in the majority of instances, alcohol test purchasing by persons under 18 years of age is not conduct to which authorisations need be applied. Any use of persons aged under 18 to make test purchases must nonetheless be subject to a risk assessment and must take account of the safety and welfare of the child.

In each instance of test purchasing, on a one-off basis, in retail premises accessible to the public, it is reasonable to assume that:

(a) surveillance is not likely to be conducted in such a way 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

(b) the test purchaser is not a CHIS because he/she does not establish or maintain a personal or other relationship with a person for the covert purpose of facilitating the obtaining of information. The one-time act of making a purchase in a shop open to the public, where there may even be no verbal exchange, cannot reasonably constitute establishing a relationship, personal or otherwise – other than a momentarily fleeting one in which no information is obtained, which could reasonably constitute an interference with the privacy of the retailer.

Those assumptions are equally valid in circumstances where it is appropriate to evidence systematic breach of licensing legislation at any given licensed premises by using a number of different test purchasers, each making a one-off purchase.

The Home Office does not believe that the use of a covert surveillance or evidence gathering device by either the child test purchaser or an observing Officer alters the position stated above. There are, however, some important qualifications to this advice. Firstly, different considerations would apply where the test purchaser had made previous visits to the premises, or is to make repeated visits, and had established or is to establish a relationship with the retailer prior to the attempted test purchase. Secondly, different considerations would apply, if the attempted test purchase is made other than from retail premises open to the public, for example from a person's home including parts of their home adjacent to retail premises.

If the use or conduct of CHIS is applied even if the test purchaser is not deemed to be CHIS, it is considered good practice to follow the RIPA authorisation requirements to ensure that -

- the safety and welfare of the test purchaser has been fully considered;
- any risk has been properly explained to, and understood by the test purchaser; and
- a risk assessment has been undertaken, covering the physical dangers including any moral and psychological aspects of the test purchaser's deployment;
- a record is kept.

In the vast majority of test purchase operations, it is likely that there will be minimal risk to the test purchaser involved. It is important that those individuals involved in the planning and conduct of test purchasing exercises avoid inciting, instigating, persuading or pressurising a person into committing an offence that, otherwise, would not have been committed.

PART 4

AUTHORISATIONS PROCEDURE FOR ACCESS TO COMMUNICATIONS DATA (ACD)

(see the Code of Practice on Acquisition and Disclosure of Communications Data)

The Council is only entitled to access subscriber data or service usage data (this does not include the contents of the communication itself).

The Council can only submit applications in relation to criminal offences that it has a statutory duty to investigate.

1. The Procedure involves four roles:

   - ☐ the Applicant (i.e. the Investigating Officer);
   - ☐ the Designated Person;
   - ☐ the SPOC (through the National Anti-Fraud Network (NAFN));
   - ☐ judicial approval by a Magistrate.

   All applications must be made online at http://www.nafn.gov.uk

2. If the application is approved, the Designated Person can authorise the accessing of communications data by one of two different methods:

   - by a Section 22 Notice which is a notice given to the postal or telecommunications operator (CSP) which requires it to collect or retrieve the data and provide it to the Council;

   - by an authorisation (referred to in this Policy Statement as an ACD authorisation) which allows the Council to collect and retrieve the data itself.

3. All applications for communications data must be made electronically through the NAFN secure online portal www.nafn.gov.uk The NAFN act as the Council's single point of contact (SPOC). This is to ensure a centralised and managed approach in making applications to obtain communications data and facilitates lawful acquisition of communications data and effective co-operation between the Council and CSPs.

   NAFN is authorised to request communications data from CSPs on behalf of a local authority, for Category B and Category C data.

   Categories:

   Category A: cell site, IEMI & incoming caller data;
   Category B: itemised billing, call diversion, data downloading, and outgoing call data;
   Category C: subscriber detail, including name and address, method of payments & customer information.

   NB: Local authorities are not able to obtain Category A data.

   The Council's Designated Persons will be notified to NAFN. Any queries regarding the use of NAFN's SPOC should be referred to the Audit Manager who acts as the Council's main point of contact with NAFN.

4. **The process**

   See the Flow Chart at Appendix B 'Process – Access to Communications Data'.

   - Applicants and Designated Persons can submit, approve and track applications through the NAFN secure online portal. The NAFN's SPOC reviews all applications for legal compliance prior to approval by the Designated Person;

- Applicants must be authorised by the Designated Person;
- NAFN will assign Applicants with a website username and password;
- NAFN will allocate a universal reference number for each application – this should be quoted on any correspondence;
- Applications should detail the necessity, purpose and proportionality of each request for information, in addition to consideration of collateral intrusion arising from the request for information. The level of detail is as required for covert surveillance and CHIS applications – (see Part 2 of this Policy Statement);
- Applications will only be approved by the Designated Person where he/she considers the application to be necessary and proportionate to the investigation;
- Following the Designated Person's approval, NAFN will prepare the court documents. It will be for the Applicant to obtain judicial approval, following the procedure detailed in Part 5 of this Policy Statement;
- The Applicant will upload the Magistrate's Order to the NAFN secure online portal;
- The NAFN will request the communications data from the CSP and provide the results to the Applicant, via the NAFN secure online portal - this data may only be further disclosed in accordance with the Council's obligations under the Data Protection Act 2018 and UK GDPR and should be stored securely;
- NAFN will liaise with a Designated Person if there are any time expiration issues which might require an application to be renewed;
- A Section 22 Notice and an ACD authorisation are valid for a maximum of one month (of the date of the Notice or Authorisation), although they can be renewed subject to judicial approval;
- A Section 22 Notice and an ACD authorisation must be cancelled if they are no longer necessary or proportionate. NAFN will effect the necessary cancellations and will notify the Designated Person and CSP. Magistrate's approval is not required for a cancellation;
- Applicants must ensure that all electronic information in relation to their applications and the data received are kept confidential and stored securely and available for inspection or audit (whether internal or external) upon request;
- A record of all applications and notices must be maintained for seven years in accordance with the Data Retention Schedule (includes authorisations, Magistrate's Order, applications granted as well as refused);
- The quality of authorisations granted from time to time may be reviewed by the Head of Legal Services , with feedback to the Designated Persons;
- NAFN may provide an annual return to the SRO containing full details of all applications submitted by the Council. It is the responsibility of the Council to then submit that report to the Interception of Communications Commissioner's Office annually.

REMEMBER – AUTHORISATIONS and SECTION 22 NOTICES WILL NOT TAKE EFFECT UNTIL JUDICIAL APPROVAL HAS BEEN SOUGHT AND GRANTED (see Flowcharts at Appendix B).

PART 5

JUDICIAL APPROVAL PROCESS

1. The Council must obtain the approval of a Magistrate (Justice of the Peace) for the use of any one of the three covert investigatory techniques available to it under RIPA - namely directed surveillance, the deployment of a CHIS and accessing communications data (ACD).

2. An approval is also required if a directed surveillance, CHIS or ACD authorisation/Section 22 Notice to use such techniques is being renewed. In each case, the role of the Magistrate to ensure that the correct procedures have been followed and the relevant factors have been taken account of. There is no requirement for the Magistrate to consider either cancellations or internal reviews.

3. The directed surveillance, CHIS or ACD authorisation/Section 22 Notice will not take effect until a Magistrate has made an order approving the authorisation/Section 22 Notice. The same considerations will apply where the Council is seeking judicial approval to renew a directed surveillance, CHIS or ACD authorisation/Section 22 Notice.

4. A renewal must be authorised prior to the expiry of the original directed surveillance, CHIS or ACD authorisation/Section 22 Notice, but it runs from the date and time of that original authorisation/Section 22 Notice.

   Directed surveillance, CHIS or ACD authorisation/Section 22 Notice may be renewed more than once, if still considered necessary and proportionate. The Council must take into account factors that may delay the renewal process e.g. intervening bank holiday weekends, availability of the authorising officer and Magistrate to grant the approval.

5. Officers representing the Council in the Magistrates' Court must ensure that they have the necessary authorisation to appear – see Scheme of Delegations to Officers.

6. Procedure – see Flowcharts at Appendix B

(a) The *original* signed authorisation for directed surveillance, CHIS or ACD authorisation/Section 22 Notice and the supporting documents (which represent information fundamental to the case) must themselves make the case and contain all the information to be relied on when making an application to the Magistrates' Court for judicial approval. It is not sufficient for the Officer representing the Council in Court, to provide oral evidence where this is not reflected or supported by the signed authorisation/notice and supporting documents.

(b) The Officer makes an arrangement with the Magistrates' Court for a single Magistrate to hear the judicial application for approval.

(c) Before the hearing, the Officer partially completes the application for judicial approval form – see Appendix B. Although the Officer is required to provide a brief summary of the circumstances of the case on this form, this is supplementary to and does not replace the need to supply the *original* directed surveillance, CHIS or ACD authorisation/Section 22 Notice as well (see para.(e) below).

(d) It is not necessary to serve the notice of the application for judicial approval on the person the subject of the authorisation for directed surveillance or CHIS or their legal representative and in the case of an ACD, on the communications service provider (CSP). The hearing before the Magistrate will not be in open court.

(e) The application for judicial approval form must be accompanied by the *original* signed directed surveillance, CHIS or ACD authorisation/Section 22 Notice and the supporting

documents and a copy. The *original* signed authorisation/Section 22 Notice and supporting documents are presented to the Magistrate after the Officer is sworn in.

A copy of the original signed authorisation/Section 22 Notice and supporting documents are retained by the Court and the original retained by the Officer.

(f) The Magistrate may note any additional information received during the course of the hearing, without requiring the application for judicial approval to be resubmitted.

(g) 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).

On the rare occasions where out of hours access to a Magistrate is required, then it will be for the Officer to make local arrangements with the Magistrates' Court. In these cases, the Officer will need to provide two partially completed applications for judicial approval forms - one copy will be retained by the Magistrate. The Officer will provide a copy of the signed form to the Court the next working day, in the same way as applications for other urgent matters.

7. Magistrate's decision

The Magistrate will first consider whether:

(a) there were reasonable grounds for the Authorising Officer/Designated Person approving the application to believe that the directed surveillance or deployment of a CHIS or an ACD was necessary and proportionate and that there remain reasonable grounds for believing so;
(b) the Authorising Officer/Designated Person was of the correct seniority within the organisation i.e. a director, head of service, service manager or equivalent as per the Regulation of Investigatory Powers (Directed Surveillance and Covert Human Intelligence Sources) Order 2010;
(c) the granting of the authorisation/Section 22 Notice was for the prescribed purpose and in relation to directed surveillance, the conditions referred to in section 9 of this Policy Statement);
(d) any other conditions set out in any order under Part 2 of RIPA are satisfied (none at present);

In addition to the above, where the authorisation is for the deployment of a CHIS, the Magistrate must be satisfied that:

(e) the provisions of section 29(5) of RIPA have been complied with. This requires the Council to ensure that there are Officers in place to carry out roles relating to the handling and management of the CHIS, as well as the keeping of records (as per the Regulation of Investigatory Powers (Source Records) Regulations 2000;
(f) where the CHIS is under 16 or 18 years of age, the requirements of the Regulation of Investigatory Powers (Juveniles) Order 2000 have been satisfied. This sets out rules about parental consent, meetings, risk assessments and the duration of the authorisation (the authorisation of such persons to act as a CHIS must come from the Director of Housing and Public Protection or in their absence, the Chief Officer and Director of Corporate Services or the Director of Growth and Community;
(g) where the application is for the renewal of a CHIS authorisation, a review has been carried out by the Council and the Magistrate has considered the results of the review.

The Magistrate may decide to

- ☐ *Approve the grant or renewal of an authorisation for directed surveillance or CHIS or in relation to ACD, approve the grant or renewal of an authorisation or the giving or renewal of a Section 22 Notice*

The grant or renewal of the RIPA authorisation will then take effect and the Council may proceed to use covert technique.

Where an ACD authorisation/Section 22 Notice has been approved by the Magistrate, a copy of the signed order must be given to the NAFN's SPOC who will then submit this and the authorisation/Section 22 Notice to the CSP.

☐ *Refuse to approve the grant or renewal of an authorisation/Section 22 Notice*

The RIPA authorisation will not take effect and the Council may not use the covert technique.

Where an application for judicial approval has been refused by the Magistrate, Officers may wish to consider the reasons for that refusal. For example, a technical error in the form may be remedied without the Council going through the internal authorisation/Section 22 Notice process again. The Council may then wish to reapply for judicial approval, once those steps have been taken.

☐ *Refuse to approve the grant or renewal and quash the authorisation/Section 22 Notice*

This applies where a Magistrate refuses to approve the grant, giving or renewal of an authorisation/Section 22 Notice and decides to quash the original authorisation/Section 22 Notice.

The Court must not exercise its power to quash an authorisation/Section 22 Notice unless the Council has had at least 2 business days from the date of the refusal in which to make representations.

The Magistrate will record his/her decision on the application for judicial approval form. The Magistrate will sign, date and endorse the time of decision. A copy of the form will be provided to the Officer.

Appeals

The Council may only appeal a Magistrate's decision on a point of law, by judicial review.

Quashing of Magistrate's approval on a complaint

The Investigatory Powers Tribunal (IPT) can investigate complaints by individuals about the use of RIPA techniques by public bodies, including local authorities. If, following a complaint to them, the IPT finds fault with a RIPA authorisation or ACD Section 22 Notice, it has the power to quash the Magistrate's approval of the authorisation or Section 22 Notice.

PART 6

COMPLAINTS

If you have any reason to believe that you have been subjected to unauthorised covert directed surveillance by the Council, or you wish to complain about any other aspect of the Council's operation under RIPA including access to communications data, then you may complain to the Council's Corporate Complaints Officer or to the Investigatory Powers Tribunal.

The Council operates an internal complaints procedure - full details are available on the Council's website. Complaints can be emailed to the complaints.officer@dartford.gov.uk or posted to:

Corporate Complaints Officer
Dartford Borough Council
Civic Centre
Home Gardens
Dartford
Kent DA1 1DR

The Investigatory Powers Tribunal can investigate anything you believe has taken place against you, your property or communications, as long as it relates to a power held by the organisation you are complaining about, under RIPA.

Investigatory Powers Tribunal
PO Box 33220
London
SW1H 9ZQ.
Tel: 0207 035 3711

Website address: www.ipt-uk.com

These procedures are mutually exclusive. However, you should first attempt to exhaust the Council's complaints procedure before complaining to the Investigatory Powers Tribunal.

Dependant upon the nature of the complaint, the Council may refer you to the Local Government and Social Care Ombudsman.

APPENDIX A – HOME OFFICE APPROVED FORMS (please see RIPA Forms)

Directed Surveillance
Directed Surveillance Authorisation Application
Directed Surveillance Authorisation Renewal
Directed Surveillance Authorisation Review
Directed Surveillance Authorisation Cancellation

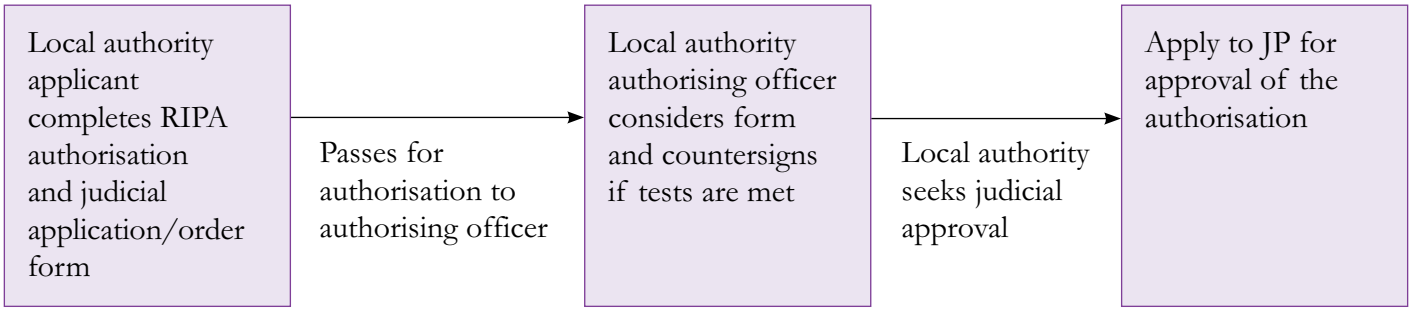
CHIS
CHIS Authorisation Application
CHIS Authorisation Renewal
CHIS Authorisation Review
CHIS Authorisation Cancellation

APPENDIX B – FLOWCHARTS

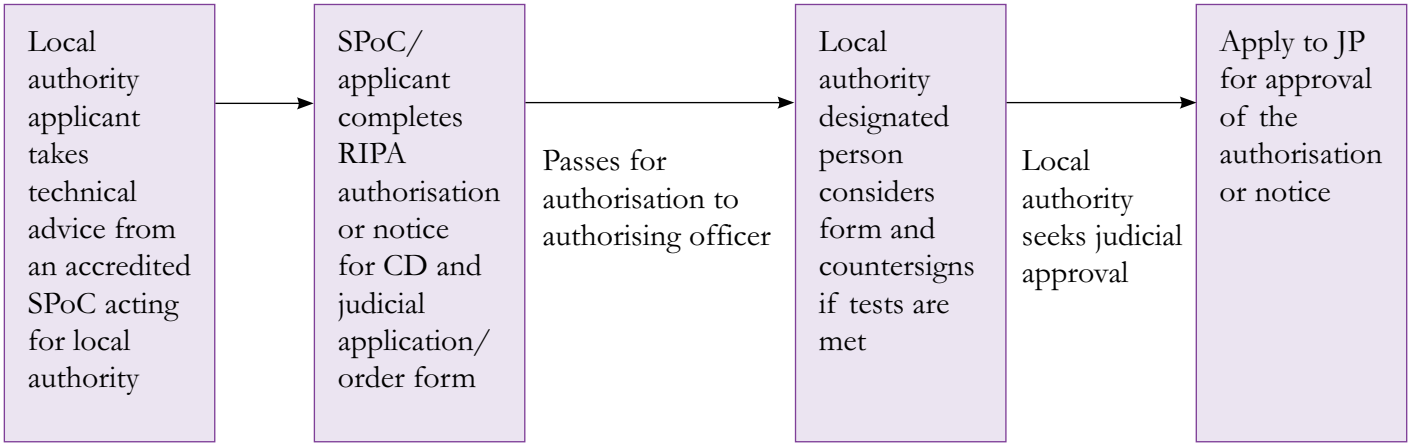
- Flowchart – RIPA/CHIS
- Flowchart – Judicial application process for applying to the Magistrates' Court
- Flowchart - Access to Communications Data

APPENDIX B

DIRECTED SURVEILLANCE / CHIS (COVERT HUMAN INTELLIGENCE SOURCE)

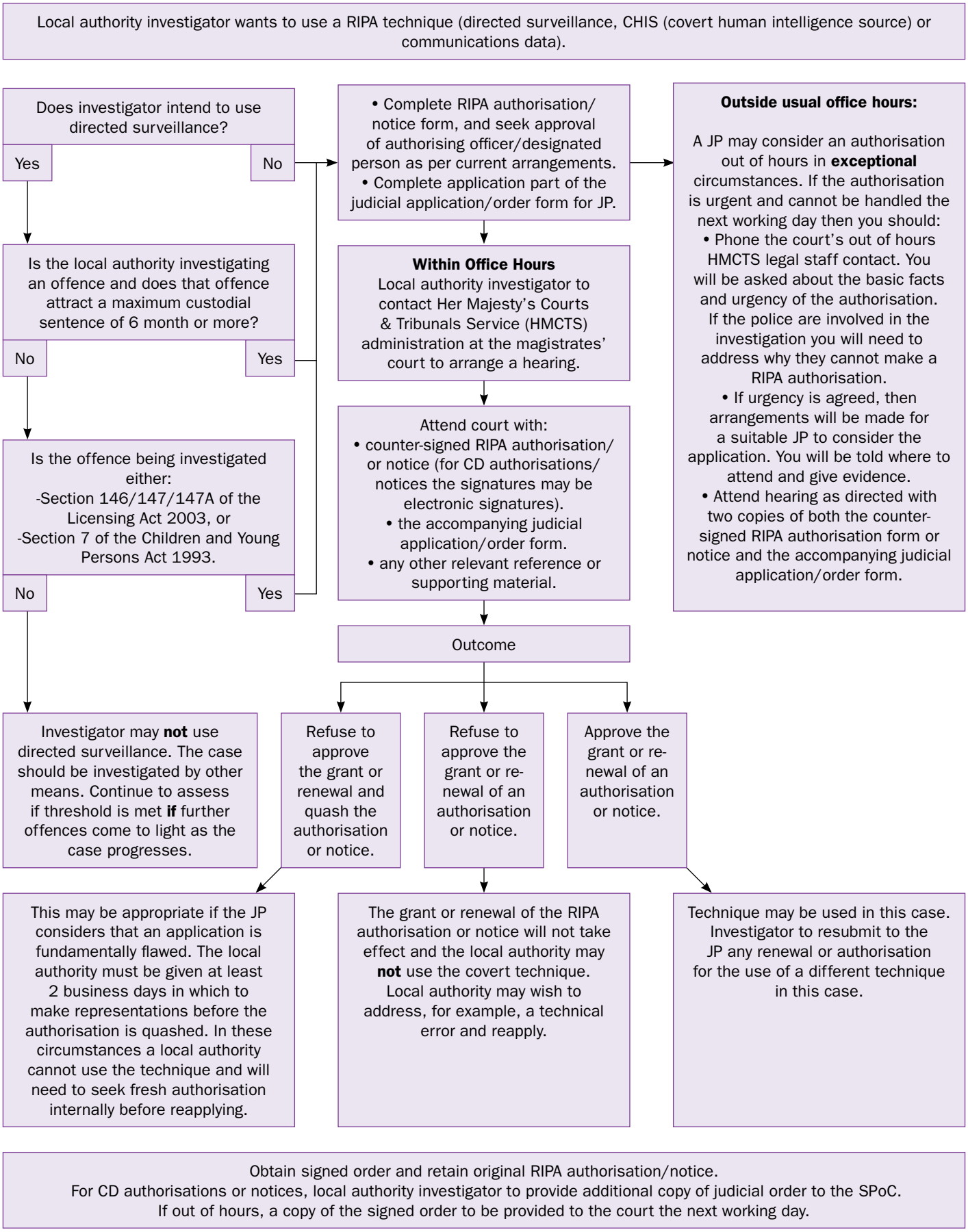


COMMUNICATIONS DATA



APPENDIX B

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



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

IN COURT HOURS

The local authority will contact Her Majesty's Courts and Tribunals Service (HMCTS) administration, who will schedule a hearing.

Local authority representative will attend the hearing with the original:

- counter-signed RIPA authorisation or notice form;
- the accompanying judicial application/order and;
- any other relevant reference material.

JP ensures that sufficient privacy is given to the hearing commensurate with the covert nature of the investigation (ie. no press, public, subject or legal representative present or court staff apart from Legal Adviser).

JP will consider papers presented by local authority, asking any additional questions in order to conclude whether an order to approve the grant of a RIPA authorisation or notice should be made. The papers by themselves make the case. It is not sufficient for the JP to rely solely on oral evidence where this is not reflected or supported by the form/papers.

OUT OF COURT HOURS

A JP may consider an authorisation out of hours, in exceptional circumstances:

- The local authority will call the court out of hours HMCTS legal staff who will ask for the basic facts and assess the urgency of the authorisation/notice. If the police are involved in the authorisation, the local authority will need to address why they cannot make the RIPA authorisation;
- If urgency is agreed, then HMCTS will arrange for local authority to attend a suitable location;
- Two copies of the forms and supporting material should be available so that one set can be retained by the JP.

The JP must be satisfied that:

- there were 'reasonable grounds' for the local authority to believe the authorisation or renewal was both 'necessary' and 'proportionate', including whether all reasonable alternatives have been considered;
- the reasonable grounds as articulated by the local authority continue to apply and the authorisation/notice continues to be necessary and proportionate;
- the local authority authorisation has been authorised by an appropriate designated person;
- there is no breach of any other restrictions imposed by order, see paragraphs 55-58, 72-73 and 83 of this guidance.

Refuse to approve the grant or renewal and quash the authorisation or notice.	Refuse to approve the grant or renewal of the authorisation or notice.	Approve the grant or renewal of the authorisation or notice.
The court must not exercise its power to quash an authorisation or notice unless the applicant has had at least 2 business days from the date of the refusal in which to make representations.	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 reapply addressing for example, a technical error.	Technique may be used. Local authority to resubmit any renewal or authorisation for the use of a different technique in this case.

Provide local authority representative with a copy of the signed order and return original RIPA form and any papers.
Legal Adviser or JP delivers copy order and authorisation to court admin office. Orders are kept securely and retained for 6 years.
Complete court hardcopy court log [do NOT enter details on LIBRA].
Court maintains a copy of the court order and will send a yearly return to MOJ.

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

Local authority:.....

Local authority department:.....

Offence under investigation:.....

Address of premises or identity of subject:.....

.....

.....

Covert technique requested: (tick one and specify details)

Communications Data ☐

Covert Human Intelligence Source ☐

Directed Surveillance ☐

Summary of details

.....

.....

.....

.....

.....

.....

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

Investigating Officer:.....

Authorising Officer/Designated Person:.....

Officer(s) appearing before JP:.....

Address of applicant department:.....

.....

Contact telephone number:.....

Contact email address (optional):.....

Local authority reference:.....

Number of pages:.....

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

Magistrates' court: .....

Having considered the application, I (tick one):

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

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

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

Notes

.....

.....

.....

.....

.....

Reasons

.....

.....

.....

.....

.....

.....

Signed:

Date:

Time:

Full name:

Address of magistrates' court:

Process - Access to Communications Data