Appendix 1

MEDWAY COUNCIL

COVERT SURVEILLANCE POLICY

REGULATION OF INVESTIGATORY POWERS ACT 2000 (RIPA)

- **DIRECTED SURVEILLANCE**
- **COVERT HUMAN INTELLIGENCE SOURCES**
- **ACQUISITION AND DISCLOSURE OF COMMUNICATIONS DATA**

Contents

PART A – Directed Surveillance and CHIS

PART B – Acquisitions and Disclosure of Communications Data

APPENDICES

POLICY

It is the policy of Medway Council to be open and transparent in the way that it works and delivers its services, including the use of surveillance. Wherever possible, overt (non-secret) investigation techniques should be used. The use of covert surveillance and sources in enforcement will be in accordance with the law. This policy sets out the guidance and procedure to be used in relation to the use of covert surveillance by Medway Council and is divided in to two sections:

1. Part A - Directed Surveillance and Covert Human Intelligence Sources
2. Part B - Acquisition and Disclosure of Communications Data.

GUIDANCE – PART A

1 Purpose

1.1 The purpose of this guidance is to explain the scope of the legislation about covert surveillance and sources, the circumstances where it applies and the authorisation procedures that must be followed.

2 Introduction

2.1 RIPA regulates the use of investigatory powers exercised by various bodies, including local authorities, and ensures that they are used in accordance with human rights. This is achieved by requiring certain investigations to be authorised by an appropriate officer before they are carried out.

2.2 The investigatory powers which are relevant to a local authority are directed covert surveillance in respect of specific operations or specific investigations and the use of covert human intelligence sources. RIPA makes it clear for which purposes they may be used, to what extent, and who may authorise their use.

2.3 Consideration must be given, prior to authorisation, as to whether or not the acquisition of private information is necessary and proportionate, i.e. whether a potential breach of a human right is justified in the interests of the community as a whole, or whether the information could be obtained in other ways.

2.4 The procedure set out in this guidance details all steps required to be carried out by Officers of the Council, or agents acting on the Council's behalf. In complying with RIPA, Officers must also have full regard to the Codes of Practice on the use of covert surveillance issued by the Home Office (see Appendix 2).

2.5 It is important to follow the guidance and procedures because RIPA

provides a defence to an accusation that there has been an infringement of a human right. Material obtained through properly authorised covert surveillance is admissible as evidence in criminal proceedings. Evidence could be excluded if the RIPA authorisation process is not followed and a court decides that it was obtained unfairly or unlawfully.

3 Legal Background

3.1 Medway Council is required to act in accordance with the provisions of a range of legislation in undertaking its duties under RIPA, including the Human Rights Act 1998 which gives effect in domestic law to one of the terms of the European Convention on Human Rights.

3.2 To be fully understood RIPA has to be seen in the wider legal context of human rights. Under Section 8 of the Human Rights Act it is unlawful for the Council to act in a manner that is incompatible with European Convention rights such as the right to respect for a person's private and family life, their home or correspondence. Such interference can be acceptable if it is "in accordance with the law". RIPA provides such a legal means of interfering with an individual's privacy providing the necessary considerations take place and the appropriate authorisations are given.

3.3 Additional legislative issues include applying the principles of Data Protection and the Council's Equalities duties.

4 When does RIPA Part II Apply?

4.1 The two principal activities that make RIPA Part II applicable to Medway Council are the use of **"Directed (Covert) Surveillance"** and the use of **"Covert Human Intelligence Sources"** (CHIS). The purpose must be to prevent or detect crime or to prevent disorder.

4.2 The provisions of RIPA apply when the Council is carrying out covert surveillance in the discharge of one of its core functions, for example trading standards investigations or child protection. There may be some circumstances where the Council considers the use of covert surveillance to prevent or detect crime in its capacity as an employer. In these circumstances it is still good practice to use the RIPA procedures and further advice should be sought from Legal Services.

4.3 The following examples illustrate circumstances when RIPA may and may not apply. Further advice is available from Legal Services.

4.3.1 The normal use of CCTV is not usually covert (secret) because members of the public are informed by signs that such equipment is in operation. However authorisation should be sought where it is intended to use CCTV to target a specific individual or group of individuals. Equally a request, for example by police to track particular individuals via CCTV recordings, may require authorisation.

4.3.2 RIPA applies to covert surveillance of a person carrying out professional or business affairs as well as of a person in their private family life.

4.3.3 When a person carries out a test purchase at a shop, this is potentially directed covert surveillance or CHIS, but it depends on the particular arrangements. Paragraph 243 of the Office of the Surveillance Commissioner's Guidance provides more details (see Appendix 2 of this guidance).

4.3.4 An immediate response to events or circumstances where it would not be reasonably practicable for a RIPA authorisation to be sought will not require authorization, specifically those events or circumstances that occur extemporarily. This does not include situations where the need for authorisation is neglected until it is too late to apply for it. See paragraph 2.23 of RIPA Covert Surveillance and Property Interference Code of Practice.

4.3.5 'Drive by' surveillance may or may not need an authorisation; it depends on the particular circumstances. It is not acceptable to prescribe a minimum number of passes before an authorisation is required.

4.3.6 With regard to 'drive by' surveillance, if it is to obtain evidence about identity of an individual then an authorisation will be required. If it is solely to observe or inspect property such as a vehicle, it will not constitute surveillance and will therefore not require an authorisation.

4.3.7 General observation that forms part of everyday duties, even if it involves use of equipment to reinforce normal sensory perception (e.g. binoculars or a camera) is not likely to be caught by RIPA. However, it will be intrusive if it consistently provides information of the same quality as might be expected to be obtained from a device actually present on the premises or in the vehicle. The quality of the image obtained rather than the duration of the observations is what is determinative.

5 What are the Different Types of Surveillance?

5.1 **Directed (Covert) Surveillance** – specifically focusing attention on an individual for the purposes of an investigation or operation conducted by Medway Council. Directed (Covert) Surveillance is carried out in a manner calculated to ensure that the person subject to the surveillance is unaware of it taking place.

5.2 **Covert Human Intelligence Sources (CHIS)** – someone (a Council officer or a member of the public) who provides information to the Council by establishing or maintaining a relationship with a person to

obtain information. The relationship is conducted in a manner to ensure that the person subject to the surveillance is unaware of it taking place.

6 Use of the Internet and Social Media

6.1. With the advances in technology making it easier, quicker and increasingly popular for individuals to share personal information on-line, the opportunities to use that information for research, investigative or other official purposes are expanding too. However, it is important to appreciate that the considerations of privacy which arise in the physical world also arise in the on-line world. In other words, there are rules and there are limits.

6.2. Simply because the content of many social media sites and other information on the internet is freely accessible does not mean that officers can openly access such information without careful regard to the constraints and requirements of the law. Repeated or systematic viewing, collecting or recording of private information from 'open' on-line sources (such as Facebook, Twitter, Snapchat and LinkedIn), including information relating to the interests, activities and movements of individuals, and others associated with them, could be regarded as a form of covert surveillance.

6.3. It is likely that individuals will have a reasonable expectation that their information is not used for surveillance purposes by public authorities and therefore may complain that their privacy and human rights have been infringed. This is the case even if their profiles are not set to private and are open to view.

6.4. Initial research of social media to establish or check some basic facts is unlikely to require an authorisation for directed surveillance, but repeated visits to build a profile of an individual's lifestyle etc. is likely to do so depending on the particular facts and circumstances. This is the case even if the information is publicly accessible because the individual has not applied any privacy settings.

6.5. Creating of fake profiles or any attempt to make 'friends' on-line for the covert purpose of obtaining information may constitute directed surveillance or, depending on the nature of the interaction or the manipulation of the relationship, a CHIS. An example would be where officers create fake profiles to investigate someone suspected of selling counterfeit goods. Note 289 of the OSC Procedures and Guidance contains more practical guidance.

7. RIPA Authorisations

7.1 The use of Directed (Covert) Surveillance or CHIS to pursue a particular line of enquiry must be properly authorised. This should ensure the admissibility of the information in evidence, and that there is minimal impact on the privacy of individuals.

7.2 Each Department must have in place **Authorising Officers** at

appropriate senior levels, who are wherever possible not involved directly in the investigation, and who will be trained to enable them to fulfill their duties under RIPA. A list of Authorising Officers is at Appendix 1 to this guidance.

7.3 Details about the process are contained in section 11.

8. The Principles of Necessity and Proportionality

8.1 The main principles that those seeking authority and those considering such authorisations must consider and address are whether the surveillance or source are **necessary** to the particular operation or enquiry and whether the surveillance or sourcing suggested is **proportionate**.

8.1.1 **Necessary** –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 of:

(a) Directed Surveillance – for the purpose of preventing and detecting conduct, which constitutes one or more criminal offences and it meets one of the following conditions set out in section 17.7 of this policy

(b) CHIS – for the purpose of preventing and detecting crime or preventing disorder

(c) Access to communications data – for the purpose of preventing and detecting crime or of preventing disorder.

8.1.2 The authorising officer will give consideration to alternative means of obtaining the information required for a directed surveillance or CHIS eg 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.

8.1.3 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.

8.1.4 Proportionate – this entails asking what the least intrusive form of the surveillance is that would result in the information sought being obtained. The method proposed must not be excessive in relation to the seriousness of the matter under investigation. it 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.

8.1.5 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.

The Home Office Code of Practice at paragraph 3.6 provides that the following elements of proportionality should be considered:

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

8.1.6 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 and should not be disproportionate or arbitrary.

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

8.2 In considering these principles it is important to take into account the risk of "collateral intrusion", i.e. intrusion on, or interference with, the privacy of persons other than the subject of the investigation. This is particularly important where there are special sensitivities, for example premises used by lawyers, doctors or priests for any form of medical or professional counselling or therapy. Steps must be taken to avoid unnecessary collateral intrusion and minimise any necessary intrusion into the lives of those not directly connected with the investigation or operation.

8.3 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.

9. RIPA Training and Awareness

9.1 Authorising Officers must have received relevant training.

10. Monitoring and Review

10.1 The Council's Monitoring Officer is responsible for implementing the activities outlined in this document, providing support to departments seeking to establish compliance and reviewing the implementation of the Policy. The programme of review will include reporting to the Council's Audit Committee.

11. Scrutiny and Tribunal

11.1 The Office of the Surveillance Commissioners (OSC) was set up to monitor compliance with RIPA. The OSC has a "duty to keep under review the exercise and performance by the relevant persons of the powers and duties under Part II of RIPA", and the Surveillance Commissioner will from time to time inspect the Council's records and procedures for this purpose.

11.2 In order to ensure that investigating authorities are using their powers properly, RIPA established a Tribunal to hear complaints from persons aggrieved by conduct. The Tribunal has power to cancel authorisations and order destruction of information obtained. The Council is under a duty to disclose to the Tribunal all relevant documentation.

PROCEDURE

12. Directed Surveillance

12.1 Definition: Section 26(2) of RIPA defines **surveillance** as being directed if it is **covert** but not **intrusive** and is undertaken:

12.1.1 for the purpose of a specific investigation or a specific operation;

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

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

12.1.4 Some of the terms above require further definition:

12.1.4.1 **surveillance** is defined at Section 48(6) of RIPA as monitoring, observing or listening to persons, their movements, conversations, activities or communications;

12.1.4.2 **covert** has a dictionary definition including secret which in this context means unknown by the person

under suspicion;

12.1.4.3 **intrusive surveillance** means involving the presence of an individual at residential premises or in someone's car, or using a surveillance device at residential premises or in someone's car. The Council cannot authorise this type of surveillance under RIPA. The Office of the Surveillance Commissioner's guidance says that gardens and driveways are not included within the definition of "residential premises";

12.1.4.4 **private information** in relation to a person includes any information relating to his/her private or family life.

12.2 Authorisation of directed surveillance: the details of which officers can authorise directed surveillance in each Department are set out in Appendix 1.

12.3 Application for directed surveillance: the following steps must be followed by officers seeking authorisation for directed surveillance (see the flowchart at Appendix 3).

12.4 DS Application Form (Part II application for Authority for Directed Surveillance) will be completed by the Investigating Officer and submitted to an Authorising Officer.

12.5 If the Authorising Officer agrees to authorise the directed surveillance, after considering the requirements of Section 28 of RIPA and the guidance in the relevant RIPA Code of Practice, then he/she will authorise the surveillance activity in writing on the DS Application Form.

12.6 **Urgent Cases**: in urgent cases authorisation may be given orally (usually by telephone) and the Authorising Officer should record this on the DS Application Form **as soon as is reasonably practicable**. Urgent authorisations should only be considered if delay would be likely to endanger life or jeopardise the operation. A delay by officers in seeking authorisation is not sufficient justification.

12.7 Duration: all written authorisations will continue until such time as they are formally CANCELLED. The duration of any directed surveillance authorisation is **three months** beginning on the date the authorisation is given. Urgent authorisation will only be given for **72 hours** beginning with the time when the authorisation was granted and will then be formally cancelled.

12.8 Review: regular reviews must be undertaken using DS Review Form to avoid authorisations running on unnecessarily.

12.9 Renewal: if required DS Renewal Form will be submitted by the Investigating Officer to apply for an authorisation renewal before the expiry of the original authorisation. The Authorising Officer will consider the renewal application and if he/she is satisfied that the criteria are still met for the authorisation will renew the authority and endorse the DS Renewal Form.

12.10 Cancellation: the officer who granted or last renewed the authorisation must cancel it if he/she is satisfied that the directed surveillance no longer meets the criteria for authorisation using the DS Cancellation Form. Authorisation must be for the statutory **three months** period. There should be appropriate reviews at a suitable time if the authorisations are to be short-lived. All authorisations should be cancelled as soon as they are no longer required; this is a statutory requirement. As soon as the decision is taken to cancel, the instruction must be given to those involved to stop all surveillance.

12.11 Original versions of the above mentioned forms should be sent to the Monitoring Officer, via Legal Services, within five working days.

12.12 It will be the responsibility of the Monitoring Officer to maintain a central record of all authorisations for directed surveillance.

13. Covert Human Intelligence Sources

13.1 Definition: Section 26(8) of RIPA defines a person as being a covert human intelligence source (CHIS) if:

13.1.1 he/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 following two paragraphs;

13.1.2 he/she covertly uses such a relationship to obtain information or to provide access to any information to another person; or

13.1.3 he/she covertly discloses information obtained by the use of such a relationship, or as a consequence of the existence of such a relationship;

13.2 For the purposes of this section a relationship is used covertly if, and only if, it is conducted in a manner calculated to ensure that one party is unaware of its purpose.

13.3 Authorisation of CHIS (Section 29): Authorisation for a CHIS can only be given by the Chief Executive (or their deputy in their absence) as set out in Appendix 1

13.4 Application for CHIS: the following steps must be followed by officers seeking authorisation for the use or conduct of a CHIS (see also flowchart at Appendix 4).

13.4.1 CHIS Application Form (Part II application for authorisation of the use or conduct of CHIS) will be completed by the Investigating Officer and submitted to an Authorising Officer.

13.4.2 If the Authorising Officer agrees to authorise the use or conduct of a covert human intelligence source, after considering the requirements of Section 29 and the guidance in the Code of Practice, then he will authorise the use of the covert human

intelligence source in writing on the CHIS Application Form.

13.4.3 **Urgent Cases**: in urgent cases authorisation may be given orally (usually by telephone) and the Authorising Officer should record this on the CHIS Application Form as soon as is reasonably practicable. Urgent authorisations should only be considered if delay would be likely to endanger life or jeopardise the operation. A delay by officers in seeking authorisation is not sufficient justification.

13.4.4 The Authorising Officer must also complete a Source Identity Form, this should include all details relating to the source as specified in Statutory Instrument 2000/2725 ensuring that the Operation Reference Number corresponds with that on the CHIS Application Form.

13.5 Special considerations:

13.5.1 **juvenile sources**: the use of juveniles as covert human intelligence sources ~~is to~~can only be authorised by the Chief Executive or his/her deputy (in his/her absence). Consideration must be given to the Requirements of the Regulation of Investigatory Powers (Juveniles) Order 2000 and the Code of Practice;

13.5.2 **vulnerable individuals as sources**: vulnerable individuals, such as the mentally impaired, should only be authorised to act as a source in the most exceptional circumstances and such authorisation ~~will~~ may only be given by the Chief Executive or his/her deputy (in his/her absence).

13.5.3 Legal advice should be sought in these circumstances.

13.6 Duration: all written authorisations will continue until such time as they are formally cancelled. A CHIS authorisation must be granted for a 12 month period, i.e. if authorised on 04.06.12 at 17:00, it will be valid until 23:59 hrs on 03.06.13. In the case of a juvenile, a CHIS authorisation may only be valid for a period of 1 month beginning on the date the authorisation is given.

13.7 Regular reviews must be undertaken using CHIS Review Form to avoid authorisations running on unnecessarily. Reviews should be as frequently as is considered necessary and practicable, but should not prevent reviews being conducted in response to changing circumstances. Juvenile sources and vulnerable individual sources will be reviewed no later than 28 days after the granting of an authorisation.

13.8 Urgent authorisation will only be given for 72 hours beginning with the time when the authorisation was granted and will then be formally cancelled unless renewed.

13.9 Renewal: the CHIS Renewal Form will be submitted by the

Investigating Officer to apply for an authorisation renewal. Before an Authorising Officer renews an authorisation, he/she must be satisfied that a review has been carried out of the use made of the source during the period authorised, the tasks given to the source and the information obtained from the use or conduct of the source. The key issue to consider is the risk involved in the operation to the source.

13.9.1 If the Authorising Officer is satisfied that the criteria for the initial authorisation continue to be met, he/she may renew the authorisation and endorse the CHIS Renewal Form.

13.10 Cancellation: the officer who granted or last renewed the authorisation must cancel it using the CHIS Cancellation Form if he/she is satisfied that the use or conduct of the source no longer satisfies the criteria or that the arrangements for oversight and management of the source are no longer in place. Authorisation should be for a 12 month period (less a day) with appropriate review dates set and should be cancelled as soon as it is no longer required; this is a statutory requirement. As soon as the decision is taken to cancel; the instruction must be given to the CHIS to stop all surveillance.

13.10 Original versions of the above mentioned forms should be sent to the Monitoring Officer, via Legal Services, within five working days.

13.11 It will be the responsibility of the Monitoring Officer to maintain a central record of all authorisations for CHIS. See paragraph 14 below for more details.

13.12 The Council is responsible for safeguarding the wellbeing of anyone authorised as a CHIS and must adhere to the following:

13.12.1 Management of Sources: every source should have a designated handler which will normally be the Investigating
13.12.2 Officer applying for the authorisation.

13.13 “Handler” means the person referred to in Section 29(5)(a) **13 Important Further Information in Relation to CHIS**

13.13.1 of RIPA who will have day to day responsibility for:

13.13.1.1 dealing with the source on our behalf;

13.13.1.2 directing the day to day activities of the source;

13.13.1.3 recording the information supplied by the source;

13.13.1.4 monitoring the source’s security and welfare.

Also every source should have a designated controller which would normally be the line manager of the Investigating

13.13.2 Officer.

13.13.3 “Controller” means the officer referred to in Section 29(5)(b) of

RIPA, responsible for the general oversight of the use of the source.

13.14 **Tasking**: tasking is the assignment given to the source by the handler or controller, asking him/her to obtain information, or to otherwise take an action leading to the obtaining of information.

13.15 When unforeseen actions or undertakings occur when a handler meets a source, or the source meets the target of an investigation, any such actions or undertakings must be recorded as soon as practicable after the event and, if the existing authorisation is insufficient, a new authorisation should be obtained before any further such action is carried out.

13.16 Original versions of the above mentioned forms should be sent to the Monitoring Officer within five working days. The Source Identity form is to be retained by the Investigating Officer and all contact with the source must be recorded. This should be sent to the Monitoring Officer only when the authorisation of the source in relation to a specified task ceases. It will be the responsibility of the Monitoring Officer to maintain a register of all authorisations granted for the retaining of covert human intelligence sources.

13.17 **Security and Welfare**: before authorising the use or conduct of a source, 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 to the target or those involved in the target activity. The ongoing security and welfare of the source, after the end or cancellation of the authorisation, should also be considered at the outset.

13.17.1 The handler is responsible for bringing to the controller's attention any concerns about the personal circumstances of the source, insofar as they might affect:

13.17.1.1 the validity of the risk assessment;

13.17.1.2 the proper conduct of the source operation;

13.17.1.3 the safety and welfare of the source.

13.17.2 Any such concerns must be brought to the attention of the Authorising Officer by the controller and a decision taken on whether or not to allow the authorisation to continue.

13.18 Record keeping:

13.18.1 Records must be maintained in such a way as to preserve the confidentiality of the source and the information provided by that source.

13.18.2 The records should contain the particulars as set out in paragraphs 3.13 and 3.14 of the Code of Practice "The Use of Covert Human Intelligence Sources" and Statutory Instrument 2000/2725. These should be made and updated by the Investigating Officer and the records or updates must be sent to the Monitoring Officer within five working days.

Repeat voluntary suppliers of information: some people provide information but do not wish to be registered as a CHIS, others repeatedly provide information that has not been sought or where the

13.19 Council does not wish to authorise the individual (e.g. because there is evidence of unreliability). However if the Council will potentially use the information there could be a duty of care to that individual, and the onus is on the Council to manage the source properly. The CHIS code of practice states that:

Public authorities must keep such human sources under constant review to ensure that they are managed with an appropriate level of sensitivity and confidentiality, and to establish whether, at any given stage, they should be authorised as a CHIS.

If it appears that a voluntary supplier of information should be authorised as a CHIS, advice should be taken from legal services as to whether authorisation should be obtained.

14 Record Keeping and Central Record of Authorisations

14.1 In all cases in which authorisation of directed surveillance and the use of a covert human intelligence source is given, the individual department is responsible for ensuring that the original documentation is sent to the Monitoring Officer who will keep it for a period of **at least three years** from the date of authorisation. These records will be available for inspection by the Office of the Surveillance Commissioner.

14.2 The Monitoring Officer will arrange for and regularly update a centrally retrievable record of all authorisations for directed surveillance in accordance with the Code of Practice. In all cases the documentation specified by the Code of Practice will be retained.

14.3 The Monitoring Officer will also arrange for and regularly update a centrally retrievable record of all authorisations for the use of covert human intelligence sources in accordance with the Code of Practice. In all cases the documentation specified by the Code of Practice will be retained.

14.4 The authorising department must ensure that appropriate arrangements are in place for the handling, storage and destruction of material obtained through the use of covert surveillance.

15 Confidential Material

15.1 Particular attention is drawn to areas where the subject of surveillance

may reasonably expect a high degree of privacy, for example where confidential material is involved. “Confidential Material” has the same meaning as it is given in Sections 98-100 of the Police Act 1997:

15.1.1 **matters subject to legal privilege** – this can include a situation where there is litigation taking place involving legal advice and also simply where a solicitor-client relationship exists for the purpose of obtaining advice or assistance in relation to rights and liabilities;

15.1.2 **confidential personal information** – this will include physical and mental health information held by healthcare professionals and spiritual counselling information held by:

15.1.1.1 Ministers of religion;

15.1.1.2 **confidential journalistic material** – this is information obtained for journalistic purposes subject to an undertaking that it will be held in confidence.

15.2 Where any authorisation is likely to result in the acquisition of or knowledge of confidential material, the authorisation can only be considered by the Council’s Chief Executive, or in their absence whoever is their deputy. Urgent oral approval can only be considered where to wait for authorisation would endanger life or jeopardise the operation. Delay caused in seeking authorisation is not justification. Legal advice should be sought where information is considered to be confidential.

15.3 The general principles applying to confidential material acquired under RIPA Part II authorisation are:

15.3.1 those handling material from such operations should be alert to anything which may fall within the definition of confidential material. Where there is doubt as to whether the material is confidential, advice should be sought from the appropriate Authorising Officer before further dissemination takes place;

15.3.2 confidential material should not be retained or copied unless it is necessary for a specified purpose;

15.3.3 confidential material should be disseminated only where an appropriate Authorising Officer is satisfied that it is necessary for a specific purpose;

15.3.4 the retention or dissemination of such information should be accompanied by a clear warning of its confidential nature. It should be safeguarded by taking reasonable steps to ensure that there is no possibility of it becoming available, or its content being known, to any person whose possession of it might prejudice any criminal or civil proceedings related to the information;

15.3.5 confidential material should be destroyed as soon as it is no

longer necessary to retain it for a specified purpose;

15.3.6 where confidential personal information or confidential journalistic material has been acquired and retained, the matter should be reported to the Commissioner or Inspector during his next inspection.

16 The product of covert activity

16.1 The Authorising Officer remains responsible for the management or destruction of the product of any covert activity. When canceling any authorisation the Authorising Officer must consider whether to retain all or part of any product and record their decision on the cancellation form.

17 Protection of Freedoms Act 2012

Introduction

17.1 The new legislation requires local authorities to obtain judicial approval for the use of any one of the three covert investigatory techniques available to them under the Act.

17.2 RIPA was designed to regulate the use of investigatory powers and to satisfy the requirements of the ECHR on its incorporation into UK law by the Human Rights Act 1998. RIPA regulates the use of a number of covert investigatory techniques, those which relate to local authorities include:

- the acquisition and disclosure of communications data (such as telephone billing information or subscriber details);
- directed surveillance (covert surveillance of individuals in public places); and
- covert human intelligence sources ("CHIS") (such as the deployment of undercover officers).

17.3 Furthermore it introduces a crime threshold, which will mean that local authorities can only grant an authorisation under RIPA for directed surveillance in particular types of criminal offences.

Restrictions

17.4 Authorising Officers may not now grant an authorisation for the carrying out of a directed surveillance unless the authorising officer can demonstrate that the proposed activity is necessary for the prevention and detection of crime and disorder (see RIPA s.81 (5)) and it meets the condition set out in the new article 7A(3)(a) or (b).

17.5 Those conditions are:

- 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

- would constitute an offence under sections:
    - 146 of the Licensing Act 2003 (sale of alcohol to children);
    - of the Licensing Act 2003 (allowing the sale of alcohol to children);
    - 147A of the Licensing Act 2003 (persistently selling alcohol to children);
    - or section 7 of the Children and Young Persons Act 1933 (sale of tobacco, etc, to persons under eighteen)

Procedure for Judicial Approval

17.6 This procedure should be read in conjunction with the guidance provided by the Home Office in relation to the judicial approval process for RIPA and the crime threshold for directed surveillance.

17.7 **An application for judicial approval:** the following steps must be followed by officers applying for a judicial order (see flow chart 3 at appendix 5)

17.8 It will be for the investigating officer to apply to the Magistrates Court. There will be a pool of investigating officers from each team:

- Audit,
- Environmental; and
- Trading Standards

The names of the investigating officers will be held on a central record, maintained by the monitoring officer. Those investigating officers will be authorised under s223 Local Government Act 1972 to appear and apply to the local Magistrates Court for judicial approval.

17.9 Following the approval by the authorising officer/designated person as per the procedure set out above the investigating officer will contact the Magistrates Court to **arrange a date for a hearing**, the officer should ask to speak to a legal advisor.

17.10 In relation to an initial **application**, the hearing should take place within **48 hours** of the investigating officer contacting the Magistrates Court. It is anticipated that these applications will be dealt with like search warrants in closed session before court starts eg at 9.45am or 1.45pm.

17.11 In relation to a **renewal**, the investigating officer should contact the court at least two weeks prior to expiration of the judicial order for a renewal application to be heard within **one week**.

17.12 There is no need for the Magistrates to consider cancellations or internal reviews.

17.13 Prior to attending the hearing, the investigating officer should ensure that s/he has:

- The original authorisation plus one copy for the court. The court should see the original but the local authority must retain this.
- Two completed copies of the application for Judicial approval
- One copy of the court order form

17.14 At the hearing itself, the investigating officer should present the evidence. The investigating officer may wish to provide other relevant reference or supporting material to the Magistrates in support of the application, either in writing or verbally, however, this does not remove or reduce in any way the duty of the authorising officer to determine whether the tests of necessity and proportionality have been met.

17.15 Judicial Approval **outside office hours**: In exceptional circumstances an authorisation may be considered and arrangements with the local Magistrates Court will be made. Investigating officers should telephone the Magistrates Court out of hours number to make the necessary arrangements.

17.16 The Magistrates may:

- **Refuse to approve the grant or renewal and quash the authorisation or notice:**
  - If the application is fundamentally flawed
  - Two business days will be given to make representations before the authorisation is quashed
  - In this case, the local authority will not be able to use the technique and will need to seek fresh authorisation internally before reapplying
- **Refuse to approve the grant or renewal of an authorisation or notice**
  - The local authority will not be able to use the technique
  - The local authority in these circumstances may wish to address any errors or technical issues and reapply
- **Approve the grant or renewal of an authorisation or notice**
  - Covert technique may be used
  - Investigating officer should resubmit to the Magistrates any renewal or authorisation for the use of a different technique in this case

REGULATION OF INVESTIGATORY POWERS ACT 2000

GUIDANCE – PART B

ACQUISITION AND DISCLOSURE OF COMMUNICATIONS DATA

Introduction

1. With effect from 5 January 2004, and in accordance with Chapter II of Part I of the Regulation of Investigatory Powers Act 2000 ('the Act'), public authorities such as Medway Council are given powers to acquire communications data. There are certain safeguards that apply in relation to the acquisition of such data. It has to be demonstrated that it is necessary for the purpose of **preventing or detecting crime or preventing disorder**; and proportionate to what is sought to be achieved by acquiring such data. If collateral intrusion is envisaged it must be demonstrated that the intrusion is justified.

2. There is a Home Office Code of Practice on the acquisition and disclosure of communications data at security.homeoffice.gov.uk/ripa/publication

3. The procedure is similar to that for the authorisation of directed surveillance and CHIS but has extra provisions and processes.

4. The purpose and effect of the procedure is the same i.e. to ensure proper consideration is given to the exercise of the powers under RIPA. The mechanism for obtaining communications data creates a system of safeguards under a detailed regulatory and legal framework. This ensures that the interference with the right of privacy of an individual through the acquisition of communications data is necessary and proportionate in any given case.

5. The Authorising Officer is the same level of officer as in the Directed Surveillance and CHIS procedure but for the purposes of this process is called a 'Designated Person'.

6. What is 'Communications data'?

6.1 Communications data is information relating to the use of a communications service e.g. postal service or telecommunications system. It is defined by
Section 21(4) of the Act and falls into three main categories: -

21(4)(a) Traffic data - where a communication was made from, to whom and when

21(4)(b) Service data– use made of service e.g. Itemised telephone records

21(4)(c)) Subscriber data – information held or obtained by operator on person they provide a service to.

6.2 Public Authorities are restricted to subscriber and service use data and only for the purpose of preventing or detecting crime or preventing disorder. Traffic data is not available to Medway Council.

7. Designated Person

7.1 A Designated Person must be at least the level of Assistant Chief Officer, Assistant Head of Service, Service Manager or equivalent.

8. Application forms

8.1 All applications must be made on a standard application form and submitted to the SPOC (single point of contact). The SPOC will ensure that the application meets the required criteria and then pass to the Designated Person for authorisation if appropriate.

9. Authorisations

9.1 Authorisations can only apply to conduct to which Chapter II of Part I of the Act applies.

9.2 In order to comply with the Code of Practice, a Designated Person can only authorise the obtaining and disclosure of communications data if:

i) It is **necessary** for any of the purposes set out in Section 22(2) of the Act. (Medway Council can only authorise for the purpose set out in Section 22(2)(b) which is the purpose of preventing or detecting crime or preventing disorder); and

ii) It is **proportionate** to what is sought to be achieved by the acquisition of such data (in accordance with Section 22(5) the Act)

9.2 Consideration must also be given to the possibility of collateral intrusion and whether any urgent timescale is justified.

9.3 Once a Designated Person has decided to grant an authorisation there are two methods by which the information can be sought from the Communications Service Provider: -

i) By **authorisation** of some person in the same relevant public authority as the Designated Person, whereby the relevant public authority collects the data itself (Section 22(3) the Act). This may be appropriate in the following circumstances:

- The postal or telecommunications operator is not capable of collecting or retrieving the communications data
- It is believed the investigation may be prejudiced if the postal or telecommunications operator is asked to collect the data itself;

- There is a prior agreement in place between the relevant public authority and the postal or telecommunications operator as to the appropriate mechanisms for the disclosure of communications data.

ii) By **notice** to the holder of the data to be acquired (s.22 (4)) which requires the operator to collect or retrieve the data. Disclosure can only be required to be made to either the Designated Person or the SPOC.

9.4 Service providers are under a duty to comply with the notice if it is reasonably practicable to do so (s.22 (6)-(8)) and non compliance can be enforced to do so by civil proceedings.

9.5 The postal or telecommunications service providers normally charge for providing this information.

9.6 There are standard forms for authorisations and notice.

9.7 There are also a number of other administrative forms the SPOC is obliged to complete in certain circumstances, although these will not always involve the requesting officer.

10. Oral authority and grading of requests

10.1 Medway Council is not permitted to authorize requests for communications data orally. Requests to Communications Service Providers are graded; grade 3 is the response level to public authorities, requests are normally dealt with within 10 working days. Grades 1 and 2 are requests by the emergency services where there is an immediate threat to life or an exceptionally urgent operation, which requires data within 48 hours.

11. Single point of contact (SPOC)

11.1 Notice and authorisations must be passed through to SPOC. The SPOC is a Home Office accredited person who deals with the postal or telecommunications operators on a regular basis and also be in a position to advise a Designated Person on the appropriateness of an authorisation or notice.

11.2 SPOCs should be in position to:

- Where appropriate, assess whether access to communication data is reasonably practical for the postal or telecommunications operator;
- Advise applicants and Designated Person on whether communications data falls under section 21 (4)(a), (b) or (c) of the Act;
- Provide safeguards for authentication;
- Assess any cost and resource implications to both the public authority and the postal or telecommunications operator.

11.3 Medway Council currently uses the National Anti-Fraud Network (NAFN) as their SPOC. NAFN is a membership organisation open to all public sector bodies providing key benefits that support members to protect the public purse and deliver effective financial governance. It is recognised by the Home Office as an expert single point of contact for data requests under the Regulation of Investigatory Powers Act 2000 for the acquisition of Communications Data.

12. Duration

12.1 Authorisations and notices are only valid for one month beginning with the date on which the authorisation is granted or the notice given. A shorter period should be specified if possible.

13. Renewal and Cancellation

13.1 An authorisation or notice may be renewed at any time during the month it is valid using the same procedure as used in the original application, Renewals now require judicial approval, following the new procedures as provided at paragraph 17 of part A of the procedure. A renewal takes effect on the date which the authorisation or notice it is renewing expires.

13.2 The code requires that all authorisations and notices should be cancelled by the Designated Person who issued it as soon as it is no longer necessary, or the conduct is no longer proportionate to what is sought to be achieved. The relevant person or telecommunications operator should be informed of the cancellation of a notice. There is no need for judicial approval upon cancellation of a notice.

14. The Protection of Freedoms Act 2012

14.1 The new legislation requires local authorities to obtain judicial approval for the use of any one of the three covert investigatory techniques available to them under the Act including communications data.

14.2 The procedure in relation to Judicial Approval should be followed as per paragraph 17 in Part A of the Guidance. Also, see flow chart 3 at appendix 5.

14.3 NAFAN have provided further guidance in relation to communication data and the Judicial process which can be found at appendix 6.

15. Retention of records

15.1 Applications, authorisations and notices must be retained by the SPOC in accordance with the Code of Practice until the Council has been audited by the Commissioner (see paragraph 10 of the Covert Surveillance Policy and Guidance).

15.2 The Monitoring Officer will maintain a centrally retrievable record of items as set out in the Code of Practice.

15.3 Applications, authorisations and all other associated documents must also be retained to allow the Tribunal (see paragraph 10 of the Covert Surveillance Policy and Guidance) to carry out its functions.

15.4 Errors which arise as a consequence of this process are determined to be either reportable errors or recordable errors and should be dealt with as specified in the Code of Practice.

15.5 Communications data, and all copies, extracts and summaries of it, must be handled and stored securely and the requirements of the Data Protection Act 1998 must be observed.

16. Oversight and Complaints

16.1 The Act establishes an Interception of Communications Commissioner whose remit is to provide independent oversight of the use of the powers contained in Part 1. The Code of Practice requires any person who uses powers conferred by Chapter II to comply with any request made by the Commissioner to provide any information he requires enabling him to discharge his functions. That will usually be in the form of an annual return to the Commissioner.

16.2 The Commissioner will also undertake a periodic inspection of all the records held by Medway Council.

16.3 The Act also establishes an independent Tribunal to investigate and decide any case within its jurisdiction. Details of the relevant complaints procedure should be available for reference from the following address:-

The Investigatory Powers Tribunal
PO Box 33220
LONDON
SW1H 9ZQ
Tel: 0207 0353711

APPENDIX 1 - Officers with authority to issue authorisations for directed surveillance

Role	Department	RIPA Authorised Officer by Job Title
Authorising Officer	RCE	Assistant Director Front Line Services
Authorising Officer	RCE~~C~~	~~Commercial Services Manager~~Head of Regulatory Services
Authorising Officer	RCE~~C~~	Head of Environmental Services ~~Manager~~
Authorising Officer	BSD	~~Audit Service Manager~~Head of Internal Audit and Counter Fraud
Monitoring Officer	BSD	Assistant Director, Legal and ~~Corporate Services~~Governance

Officers with authority to issue authorisations for CHIS or Confidential Information

Role	Department	RIPA Authorised Officer by Job Title
Authorising Officer	All	Chief Executive (or in their absence their Deputy)

APPENDIX 2 – Codes of Practice

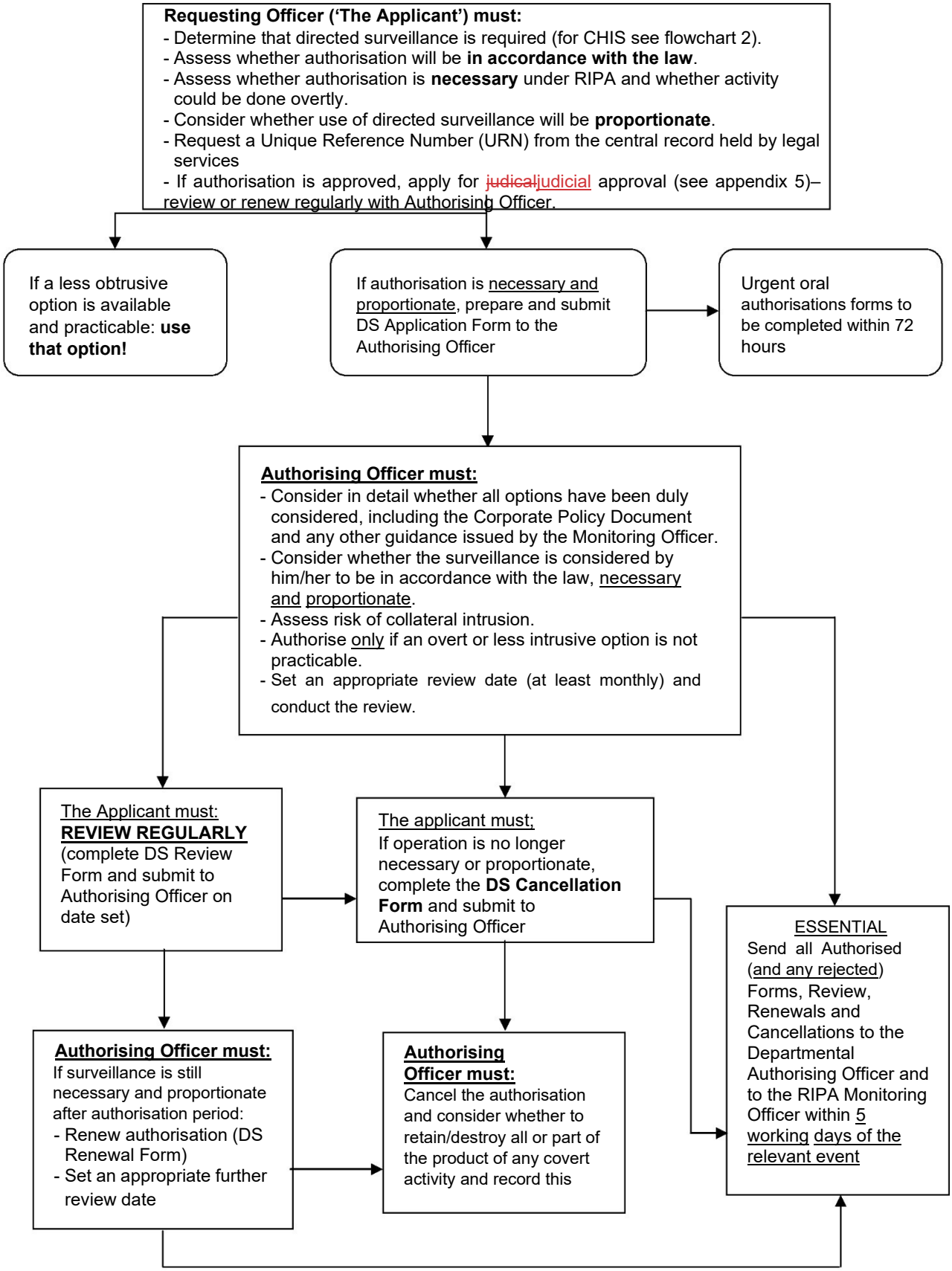
Home Office Covert Surveillance Code of Practice

Home Office Covert Human Intelligence Source Code of Practice

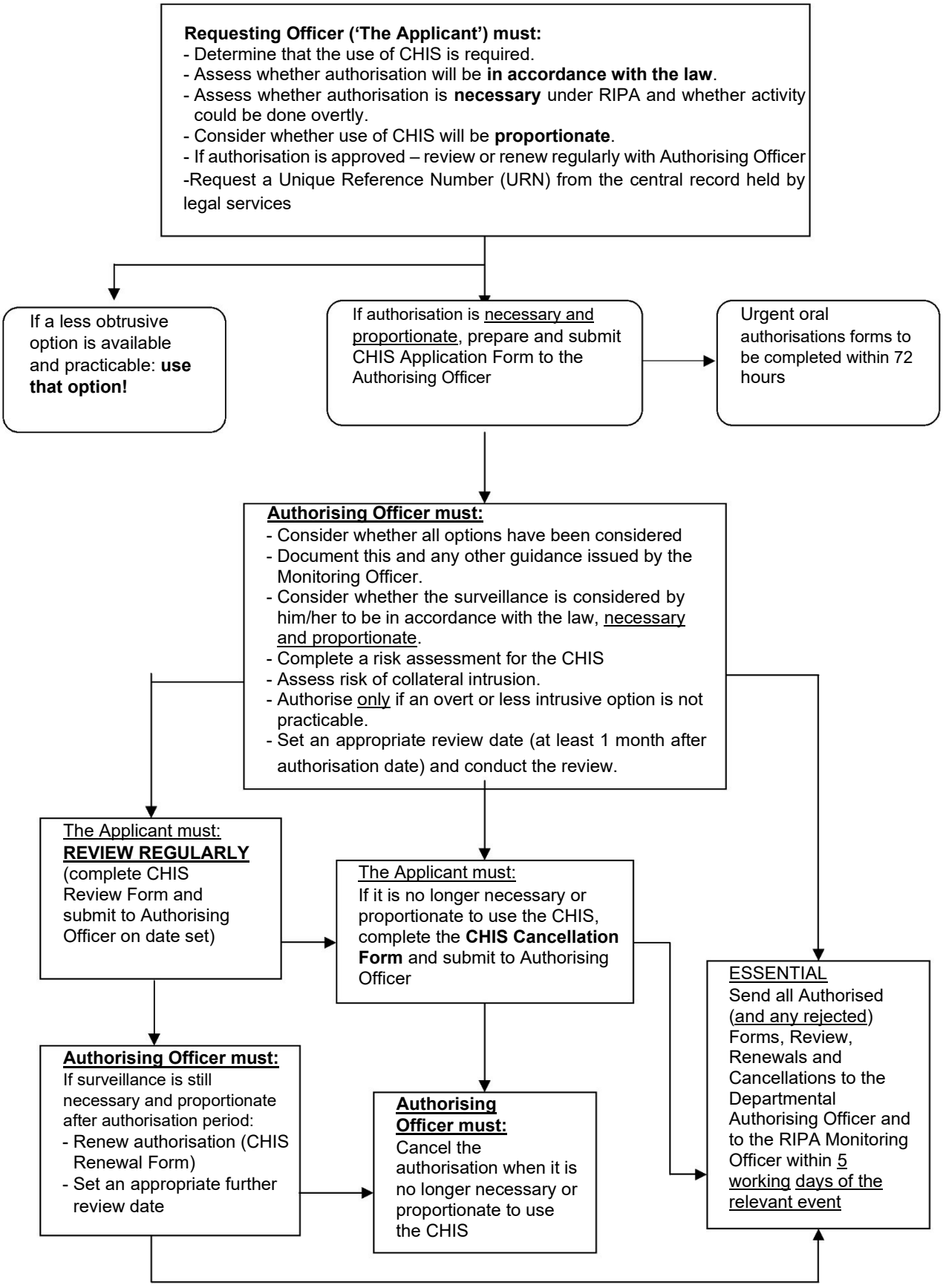
Office of the Surveillance Commissioners Procedures and Guidance – oversight arrangements for covert surveillance and Property Interference conducted by public authorities

Protection of Freedoms Act 2012 – Changes to provisions under the Regulation of Investigatory powers Act 2000 (RIPA) - Home Office guidance to local authorities in England and Wales on the judicial approval process for RIPA and the crime threshold for directed surveillance (October 2012)

APPENDIX 3 – RIPA FLOWCHART 1: AUTHORISING DIRECTED SURVEILLANCE

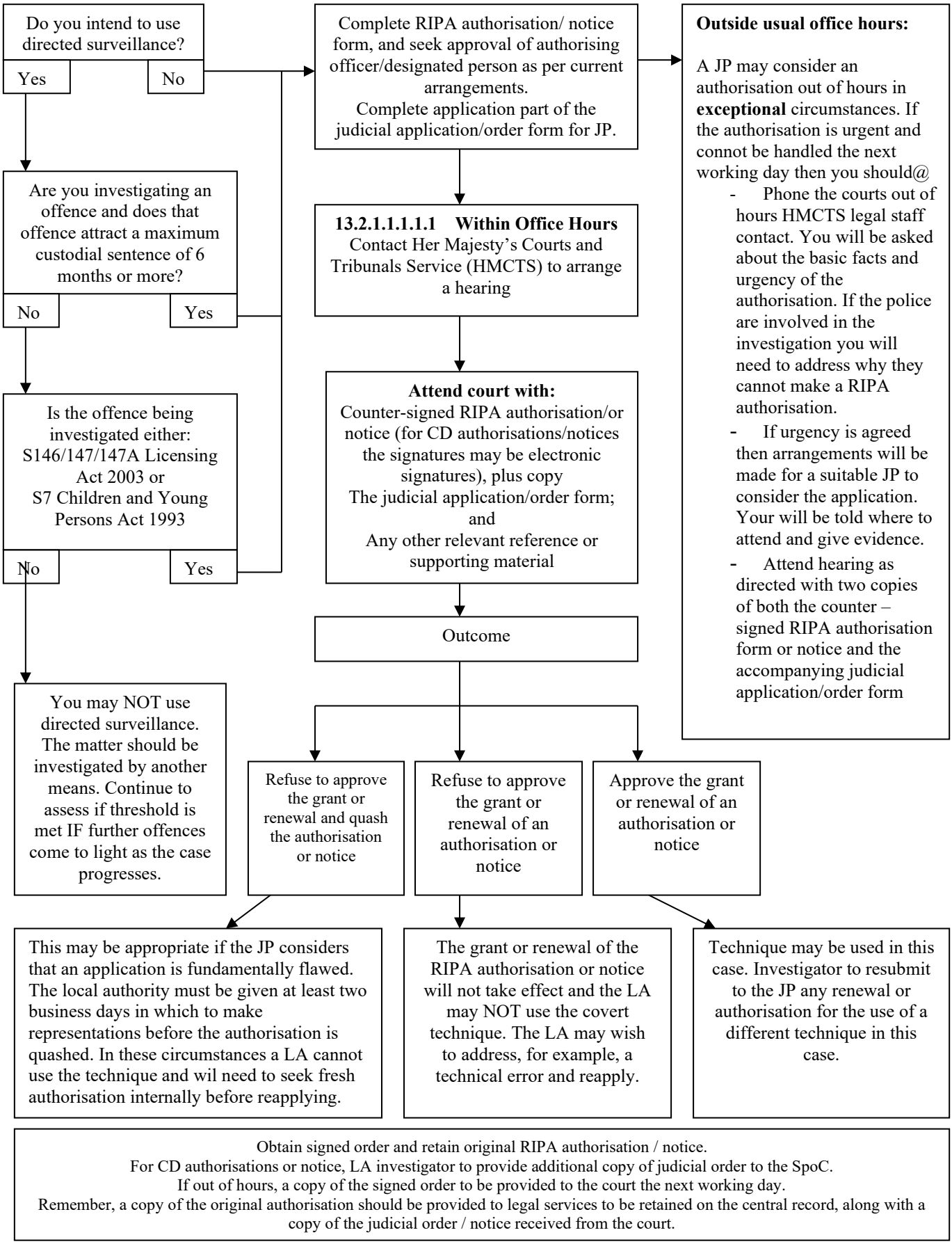


APPENDIX 4 – RIPA FLOWCHART 2: AUTHORISING COVERT HUMAN INTELLIGENCE SOURCES



APPENDIX 5 – RIPA FLOWCHART 3: APPLICATION TO A JUSTICE OF THE PEACE SEEKING AN ORDER TO APPROVE THE GRANT OF A RIPA AUTHORISATION OR NOTICE

Authorised Investigating Officers (authorised under s223 Local Government Act) to follow the procedure as set out below:



Obtain signed order and retain original RIPA authorisation / notice.
For CD authorisations or notice, LA 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.
Remember, a copy of the original authorisation should be provided to legal services to be retained on the central record, along with a copy of the judicial order / notice received from the court.

APPENDIX 6 – GUIDANCE PROVIDED BY NAFN

Court Hearing Guidance

You may already be familiar with making applications to the Magistrates for orders in connection with the investigation of offences. All courts have local practices and if the practice at your local court is different you should follow the local practice.

1. Before the hearing

Read through the authorisation and the application form for Judicial Approval thoroughly. You are welcome to amend the application form supplied by NAFN but the authorisation itself should not be amended once it has been approved by the Designated Person.

Ensure you have: **The original authorisation plus one copy.**
Two copies of the application for Judicial approval
One copy of the Court Order form.

Be prepared to explain everything to the Magistrate – remember they may never have seen an application like this before. Try and anticipate what questions the Magistrate might ask.

Check if it is necessary for your Head of Legal Services to authorise you to appear in Court.

Make sure the Court know you are coming in advance.

2. At the hearing

You should address the Magistrate as 'Sir' or 'Ma'am'. They may be accompanied by a legal adviser who will be a lawyer. The public should not be present during the application. This is important because anything heard by the public might get back to the person you are investigating.

After introducing yourself you may be asked to swear an oath (or make an affirmation). This is a matter for the Magistrate's discretion. In general it is necessary to be sworn in if what you say is going to be treated as formal evidence. If, however, what you say is a presentation about the authorisation then it is not strictly necessary for you to be sworn in. Leave this to the Magistrate. If you are asked to swear an oath you can choose to affirm instead if you object to swearing on the Bible/Holy book. Legally there is no difference between an oath or an affirmation. It is a matter of your own personal preference/religious belief. Magistrates should be able to accommodate all religious requirements.

The Magistrate may not be familiar with RIPA. It is helpful if you offer to talk them through the application, or the entire authorisation. The Magistrate may not find this necessary but they will generally appreciate the offer.

3. If everything goes well

Ask the Magistrate to sign the order. You need to keep the original authorisation and the original signed order. The Magistrate keeps a copy of everything for the Court records. Ensure that the scanned signed application form and order are returned to NAFN.

4. If the Magistrate is not happy to approve the authorisation

In most cases it is likely that the Magistrate will be happy to approve the authorisation.

However, if the Magistrate is not happy to authorise try to get as much information as possible as to why. It might be helpful to ask them if there is any further information which can be provided in support to help persuade them in future. You cannot amend the authorisation without getting it approved again by the Designated Person, but you can amend the application for Judicial approval. You can also provide further evidence to the Magistrate outside the application – if they agree to this.

If the Magistrate considers quashing the authorisation they must adjourn the application for at least two working days to give you a chance to make further representations. Although this isn't in RIPA, it is a strict legal requirement in the Criminal Procedure Rules (rule 6.28).

Whatever the outcome you should take the original authorisation with you when you leave.

5. Need further advice

If you are not sure of what to do next or need further advice contact NAFN who will be able to assist and direct your query accordingly.

NAFN UK North NAFN UK South
Telephone: 0161 342 3727 **Telephone:** 01273 291322
Email: spoc@nafn.scn.gov.uk **Email:** spoc@nafn.scn.gov.uk