Corporate Policy And Procedures Document

On

The Regulation Of Investigatory Powers Act 2000 (RIPA) (as amended, including changes from the Investigatory Powers Act 2016)

Version:	October 2019
Document Owners:	Internal Audit Manager
Approved By:	Corporate Management Team

ARUN
DISTRICT COUNCIL

1.0 Introduction

1.1 This Corporate Policy and Procedures Document is based upon the requirements of the Regulation of Investigatory Powers Act 2000 (RIPA), as amended by:-

- a number of Statutory Instruments
- the Protection of Freedoms Act 2012
- the Investigatory Powers Act 2016 (as further amended by the Data Retention and Acquisition Regulations 2018)

and the revised Home Office Codes of Practice on:-

- Covert Surveillance and Property Interference
- Covert Human Intelligence Sources (CHIS)
- Acquisition and Disclosure of Communications Data.

1.2 RIPA and this document are important for the efficient and effective operation of the Council's actions with regard to covert surveillance, covert human intelligence sources and the acquisition / disclosure of communications data. This policy and procedures document will be reviewed by the Council's Internal Audit Manager and the Audit & Governance Committee annually. Where references are made to RIPA throughout this document, then this should also include IPA (in relation to communications data).

1.3 All staff directly employed by Arun District Council (ADC) and external agencies working for the Council are covered by the Act for the time they are working for the Council. Therefore, all external agencies must comply with RIPA and any relevant actions carried out by such agencies on the Council's behalf must be properly authorised by one of the Council's designated Authorised Officers. The Authorised Officers are those whose names appear in Appendix E.

1.4 If the correct procedures are not followed, or all required authorisations are not obtained, then evidence gathered may be deemed inadmissible for enforcement or other purposes and activities may be unlawful, leaving the Council open to regulatory or legal action. It is therefore vitally important that all Officers involved in work to which RIPA may apply are fully conversant with the requirements of the Act and the Codes of Practice.

1.5 Officers do, however, on occasion need to use covert surveillance and / or obtain communications data to carry out statutory and non-statutory functions. In order to ensure this is undertaken in a fair and lawful way, and in accordance with the Human Rights legislation, Arun District Council is committed to complying with the Regulations of Investigatory Powers Act 2000 (RIPA), as amended. Therefore, covert surveillance and the obtaining of communications data will only take place if the Officer responsible for management of the investigation has obtained the necessary authorisation within the Council by the Chief Executive, Group Head of Council Advice & Monitoring or an appropriate Authorising Officer.

1.6 From 1 November 2012, the Protection of Freedoms Act 2012 imposes additional restrictions on the activities that can be subject to directed surveillance and also requires that all such RIPA activities are subject to judicial approval, before commencement. The Investigatory Powers Act replaces the RIPA powers for communications data and, from June 2019, requires that any such requests be independently authorised by the Office for Communications Data Authorisations (OCDA).

1.7 The Council will comply with the Codes of Practice issued by the Secretary of State and has established procedures by which the powers can be authorised, detailed later in this document. Links to the Home Office Codes of Practice can be found on the Council's SharePoint under Internal Audit / RIPA. Appropriate standard forms have also been provided by the Home Office (listed in Appendix D) and these are available to relevant Officers via the Council's SharePoint.

1.8 The Council aims to ensure that relevant staff understand the scope of RIPA in relation to their area of work. All staff whose jobs are likely to involve surveillance work will undertake training on the Act and its implications. This training should enable these staff to understand the procedures and safeguards, and to minimise the risk that staff will attempt to undertake investigations using methods incompatible with the requirements of RIPA.

1.9 Careful consideration must always be given to alternative, legal methods of gathering information before seeking authorisation under RIPA. This is to ensure that the use of surveillance is an effective way of obtaining evidence and that the Council is able to demonstrate that RIPA use is both necessary and a proportionate response to the circumstances of each case.

1.10 The Chief Surveillance Commissioner has previously advised that all public authorities empowered to use RIPA should have in place a corporate policy on the use of social media in investigations - while social networking sites may be accessed as part of investigations, there must be corporate direction and oversight. This must include consideration of whether such activities constitute covert directed surveillance or the use of a confidential human intelligence source as defined within RIPA and which must therefore be conducted in line with this policy. A separate 'Guidance on the Use of Social Media in Investigations' document provides further information in this regard.

1.11 RIPA requires that a central retrievable register be held by the Council and is regularly updated whenever an authorisation is granted, reviewed or cancelled. This record shall be kept by the Internal Audit Manager and shall be available to the relevant Commissioner or an Inspector from the Investigatory Powers Commissioner's Office (IPCO), which assumed responsibility from the former Office of Surveillance Commissioners (OSC) in September 2017, upon request. The central register will be reviewed at three monthly intervals, to ensure compliance with this Policy and to promulgate examples of best practice. These records should be retained for 3 years following the end of an authorisation and be available for review at the next triennial inspection by the Investigatory Powers Commissioner's Office. Once the inspection has been completed, historic records reviewed may be destroyed.

1.12 As part of the review process, the Internal Audit Manager will periodically request confirmation from Service area senior management that they:-

- (and their staff) are aware of current RIPA legislation and processes
- have authorised and registered any RIPA use, in accordance with this Policy
- have not undertaken any activities covered by RIPA (as contained in this Policy and the appropriate Home Office Codes of Practice) without the necessary authorisation and judicial approval.

1.13 In addition, each Service area shall keep a record of authorisations and / or use of a source. Service departments may keep their copies of the authorisations for longer where they may be required for a future prosecution or other legal intervention - however, they must destroy their copies as soon as they are no longer required.

1.14 There is no provision within the Act which prevents material obtained from one properly authorised source being used in other investigations. The Council will, however, ensure that arrangements are in place for the handling, storage and destruction of material obtained though this avenue. Authorising Officers must ensure compliance with the data protection requirements and the Council's Data Protection Policy in relation to the handling and storage of material.

2.0 Explanation of the Act and Codes of Practice

2.1 The Regulation of Investigatory Powers Act 2000 (RIPA), as amended, is concerned with the regulation of surveillance by public authorities, such as Arun District Council, in the conduct of their legitimate business. Surveillance is part of modern life, but had not previously been the subject of formal statutory control. The 2010 guidance from the Home Office, and the further restrictions / requirements for judicial approval of RIPA use contained in the Protection of Freedoms Act 2012, take into account public unease over adverse publicity regarding the apparent misuse of the powers by a minority of Local Authorities to deal with seemingly trivial matters. The latest legislation and codes of practice provide much clearer guidance as to when the use of surveillance is appropriate and when it is not.

2.2 RIPA was enacted to regularise the situation and to ensure that, when conducting surveillance, public authorities have regard to the Human Rights Act 1998 and Article 8 of the European Convention of Human Rights (the right to a private and family life) regulated by RIPA.

2.3 Part 4 of the Act provides for independent judicial oversight of powers where necessary. It also established a Tribunal as a means of redress for those who wish to complain about the use of the powers. The Act also provided for the Secretary of State to issue Codes of Practice covering the use of the powers covered by the Act.

2.4 The Secretary of State has issued revised Codes of Practice (as noted in section 1.1 above) and guidance on the changes from the Protection of

Freedoms Act 2012 and the Investigatory Powers Act 2016, which should be given careful consideration by all Officers involved in RIPA-related activities.

2.5 The Investigatory Powers Commissioner's Office (IPCO) keeps under review the performance of functions relating to covert surveillance and makes periodic inspections for these purposes. The OSC (now IPCO) periodically publishes a Procedures and Guidance document on the oversight arrangements for covert surveillance and property interference conducted by public authorities.

2.6 Arun District Council is defined as an authority to which RIPA applies by virtue of Section 1 of the Local Government Act 1999. The forms of surveillance that ADC is entitled to authorise are:-

- covert directed surveillance
- the use of covert human intelligence sources (informants), known as CHIS

from 1 November 2012, any such RIPA activity to be conducted by the Council must also have judicial approval before commencement

- the acquisition and disclosure of communications data

from 1 November 2018, a serious crime threshold will be applied and from June 2019 applications will require independent authorisation from the Office for Communications Data Authorisations (OCDA).

2.7 <u>Covert Directed Surveillance</u>

2.7.1 Covert Directed Surveillance means surveillance which is carried out in such a way that the person(s) subject to it is unaware that it is or may be taking place.

2.7.2 It is essentially covert surveillance in places other than residential premises or private vehicles – surveillance in these is termed 'intrusive' and cannot be conducted by local authorities under the RIPA framework.

2.7.3 Surveillance is directed if it is:-

- covert, but not intrusive;
- undertaken for the purposes of a specific investigation; and
- conducted in such a way as to obtain private information about a person other than by way of an immediate response to events or circumstances.

2.7.4 As a result of the Protection of Freedoms Act, from 1 November 2012 Directed Surveillance authorisations will have a crime threshold applied:-

- local authorities can only authorise use of directed surveillance under RIPA to prevent or detect criminal offences that are either punishable, whether on summary conviction or indictment, by a maximum term of at least 6 months' imprisonment or are related to the underage sale of alcohol and tobacco
- local authorities cannot authorise directed surveillance for the

purpose of preventing disorder, unless this involves such a criminal offence

- this will continue to allow the use of directed surveillance in more serious cases, as long as the requirements for necessity, proportionality and prior JP approval have been met. Examples of this could include more serious criminal damage, dangerous waste dumping and serious or serial benefit fraud
- a local authority may not now authorise the use of directed surveillance under RIPA to investigate disorder that does not involve criminal offences or to investigate low-level offences which may include, for example, littering, dog control and fly-posting
- at the start of an investigation, officers will need to satisfy themselves and the JP that what they are investigating is a criminal offence. If, during the investigation, it becomes clear that the activity being investigated does not constitute a criminal offence or that it would be a less serious offence that does not meet the threshold, the use of directed surveillance should cease. If a directed surveillance authorisation is already in force it should be cancelled
- while local authorities will no longer be able to use directed surveillance in some cases where it was previously authorised, this does not mean it will not be possible to investigate these areas with a view to stopping offending behaviour. The RIPA Code of Practice on covert surveillance makes it clear that routine patrols, observation at trouble 'hotspots', immediate response to events and overt use of CCTV are all techniques that do not require RIPA authorisation
- the manner in which evidence is collected should be considered as to whether it may be considered 'routine'. If there is any doubt as to whether RIPA applies to activities being proposed, then advice should be sought from the Council's Legal Services or Internal Audit areas.

2.8 Covert Human Intelligence Source (CHIS)

2.8.1 A person is a Covert Human Intelligence Source (CHIS) if they establish or maintain a relationship with another person in order to:-

- covertly obtain information;
- provide access to information to a third party; or
- covertly disclose information obtained by the use of such a relationship and the other person is unaware that the purpose of the relationship is one of the above.

2.9 Communications Data

Communications Data means any traffic or any information that is being or has been sent by a telecommunications system or postal system, together with information about the use of the system made by any person e.g. e-mails, letters, telephone calls (now covered by the Investigatory Powers Act 2016).

2.10 General Observation

2.10.1 It is important to distinguish between the types of surveillance and information gathering regulated by RIPA, and normal general observation in the course of discharging the Council's functions. It is acknowledged that low-level activity will not actually be regulated under the provisions of RIPA. The Covert Surveillance Code of Practice gives the following examples of this kind of general observation:-

- patrolling to prevent crime and disorder
- visiting of premises by Officers as part of their enforcement function

2.10.2 Even when this might involve using binoculars or cameras, the Code states that this sort of activity is general observation as it does not involve the "systematic surveillance of an individual".

3.0 Human Rights and RIPA

3.1 The Human Rights Act 1998 requires the Council, and any organisation working on its behalf, to respect a person's private and family life, their home and correspondence (pursuant to article 8 of the European Convention on Human Rights).

3.2 The Convention qualifies this right so that in certain circumstances the Council may interfere in that person's right if that interference is:-

- in accordance with the law;
- necessary; and
- proportionate.

3.3 RIPA provides a statutory mechanism for the authorising of covert surveillance, the use of a Covert Human Intelligence Source (CHIS) and the acquisition of communications data. It also permits Public Authorities to compel telecommunications and postal companies to obtain and release communications data to them. This can take place only in certain circumstances. As the Convention seeks to ensure that any interference with a person's rights under Article 8 is necessary and proportionate, RIPA seeks to ensure that the human rights of individuals and the public interest are balanced and this has been strengthened by the Protection of Freedoms Act 2012.

3.4 Surveillance is an intrusion into the privacy of the citizen. Arun District Council will not undertake surveillance unless it is:-

i. necessary;
ii. proportionate; and
iii. properly authorised (both by an Authorising Officer and a JP, following judicial review).

3.5 Where there are alternate legal means of obtaining the information, which is less intrusive on the rights of the citizen, we will always take that alternative course rather than undertake surveillance.

3.6 Surveillance will always therefore be conducted within the constraints of the authorisation. It will cease when the evidence sought has been obtained, or when it becomes clear that the evidence is not going to be obtained by further surveillance. At this point the authorisation should be cancelled.

3.7 All Officers of ADC involved in applying for, authorising or undertaking surveillance will undertake this in line with the requirements set out in RIPA (as amended) and the Codes of Practice.

3.8 Covert surveillance which is properly authorised will, as long as it is carried out in accordance with the terms of the authorisation, be legitimate. The authorisation would provide a defence to any challenge under the Human Rights Act.

3.9 Confidential Information

3.9.1 The 2000 Act does not provide any special protection for "confidential information". Nevertheless, particular care should be taken in cases where the subject of the investigation might reasonably expect a high level of privacy, or where confidential information is involved. Confidential information consists of matters subject to legal privilege, confidential personal information (medical or religious / spiritual information) or confidential journalistic material. For example, extra care should be given where, through the use of surveillance, it would be possible to acquire knowledge of discussions between a minister of religion and an individual relating to the latter's spiritual welfare, or where matters of medical or journalistic confidentiality or legal privilege may be involved.

3.9.2 In cases where, through the use of surveillance, it is likely that knowledge of confidential information will be acquired, the use of surveillance is subject to a higher level of authorisation. Only the Chief Executive can authorise any application where confidential information is likely to be acquired,

4.0 The General Data Protection Regulation (GDPR) / Data Protection Act 2018 (DPA) and RIPA

4.1 The EU's General Data Protection Regulation (GDPR) and the Data Protection Act 2018 have replaced the UK's Data Protection Act 1998 in order that data protection law is generally identical across the EU. The GDPR contains a set of 6 principles, which state that personal data, which includes personal data from covert surveillance techniques must be:-

- processed lawfully, fairly and in a transparent manner ('lawfulness and transparency');

- collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes *'purpose limitation');
- adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation');
- accurate and, where necessary, kept up to date ('accuracy');
- stored for no longer than is necessary ('storage limitation');
- kept secure and protected from unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ('integrity and confidentiality').

4.2 All authorisations, notebooks, logs and other ancillary documentation will be retained for a period of three years and will be made available for any appropriate management or regulatory inspection.

5.0 Surveillance - What Is It?

5.1 Surveillance includes:-

- monitoring, observing, listening to persons, watching or following their movements, listening to their conversations, and other such activities or communications
- recording anything mentioned in the course of authorised surveillance
- surveillance by or with the assistance of appropriate surveillance devices.

5.2 Overt or Convert Surveillance?

5.2.1 Overt

Most of the surveillance carried out by the Council will be conducted overtly. There will be nothing secretive, clandestine or hidden about it. In many cases Officers will be behaving in the same way as members of the public, and will be going about Council business openly e.g. inspecting food premises, undertaking site visits, home visits for benefit claims / reviews.

5.2.2 Covert Surveillance

Covert surveillance is carried out in a manner intended to ensure the person(s) subject to the surveillance is unaware that it is taking place (Section 26 (9)(a) of RIPA). It is not classed as necessary or proportionate if there is reasonably available overt means of finding out the information. There are two types of covert surveillance:-

- Directed
- Intrusive.

5.2.3 Directed Covert Surveillance

This is surveillance that is:-

i. covert; and

ii. non-intrusive.

5.2.4 Immediate Response Surveillance

Covert surveillance that is likely to reveal private information about a person but is carried out by way of an immediate response to events, such that it is not reasonably practicable to obtain an authorisation under the 2000 Act, would not require a directed surveillance authorisation. The 2000 Act is not intended to prevent law enforcement officers fulfilling their legislative functions.

5.2.5 Surveillance on Business Premises

The fact that covert surveillance takes place in a business premises does not mean it cannot result in the obtaining of private information about a person. The way a person conducts their business can also reveal information about their private life and others e.g. family members.

5.2.6 CCTV

CCTV cameras do not normally require authorisation. If the camera is used for a specific purpose which involves surveillance on a particular individual, authorisation will be required.

5.2.7 Aerial Covert Surveillance

Where surveillance using unmanned aircraft (colloquially known as 'drones') is planned the Home Office Code requires that consideration should be made to determine whether a surveillance authorisation is appropriate. In considering whether the surveillance should be regarded as covert, account should be taken of the reduced visibility of a craft or device at altitude.

5.3 Intrusive Surveillance

5.3.1 Directed surveillance is non-intrusive. Intrusive surveillance takes place when it is:-

i. covert;
ii. relates to residential premises and private vehicles; and
iii. involves the presence of a person in the premises / vehicle.

5.3.2 Surveillance equipment mounted outside the premises will not be intrusive, unless the device consistently provides information of the same quality and detail as might be expected if it were in the premises / vehicle.

5.3.3 Intrusive surveillance can only be carried out by the Police and other law enforcement agencies.

6.0 Covert Human Intelligence Source (CHIS)

6.1 Definition

A CHIS is someone who establishes or maintains a personal or other relationship with a person for the covert purposes of helping the Council by:-

- covertly using such a relationship to obtain information or to provide access to any information to another person
- covertly disclosing information obtained by use of such a relationship or as a consequence of the existence of such a relationship.

The relationship will be for a covert purpose only if it is conducted in a manner that is calculated to ensure that one of the parties to the relationship is unaware of the purpose.

6.2 Information from the Public

6.2.1 Where members of the public volunteer information or provide it through a contact number set up to receive such information e.g.:-

- benefit fraud hotline
- neighbour complaining of possible planning permission breach,

RIPA will not apply (as long as no covert relationship is established under the provisions of section 6.1 above).

6.2.2 Determining the status of an individual or organisation providing information is a matter of judgement by the public authority. Public authorities should avoid inducing individuals to engage in the conduct of a CHIS either expressly or implicitly without obtaining a CHIS authorisation. If there is any doubt as to whether RIPA applies to activities being proposed, then advice should be sought from the Council's Legal Services or Internal Audit areas.

6.3 What Must Be Authorised

6.3.1 Use

The use of a CHIS involves any action on behalf of a public authority to induce, ask or assist a person to engage in the conduct of a CHIS, or to obtain information by means of the conduct of a CHIS.

6.3.2 Conduct

The conduct of a CHIS is any conduct that falls within the definition of a CHIS above.

6.3.3 Handlers and Controllers

Public authorities should ensure that arrangements are in place for the proper oversight and management of CHIS, including appointing individual officers as defined in section 29(5)(a) and (b) of the 2000 Act for each CHIS.

The person referred to in section 29(5)(a) of the 2000 Act (the "handler") will have day to day responsibility for:-

- dealing with the CHIS on behalf of the authority concerned;
- directing the day to day activities of the CHIS;
- recording the information supplied by the CHIS; and
- monitoring the CHIS's security and welfare.

The handler of a CHIS will usually be of a rank or position below that of the authorising officer.

The person referred to in section 29(5)(b) of the 2000 Act (the "controller") will normally be responsible for the management and supervision of the "handler" and general oversight of the use of the CHIS.

6.3.4 Authorisation

Prior authorisation will be required by an Authorising Officer and, from 1 November 2012, from a JP. An authorisation will be required covering:-

- Use - the steps taken by a public authority in relation to the use of a CHIS, including asking or assisting a person to act as a CHIS and the decision to use a CHIS in the first place
- Conduct – the steps taken by the CHIS on behalf, or at the request, of a public authority.

Most CHIS authorisations will be for both use and conduct. Care should be taken to ensure that the CHIS is clear on what is / is not authorised at any given time and that all the CHIS's activities are properly risk assessed.

6.4 Special Circumstances

6.4.1 Juveniles (Under 18) and Vulnerable Individuals

There are special safeguards with regard to the use of such individuals. On no occasion can a child under 16 years of age be authorised to give information against his or her parents or any person who has parental responsibility for him / her. Only the Chief Executive (or a designated Director, acting as the Head of Paid Service in his absence) is duly authorised to use such vulnerable individuals as there are onerous requirements for such authorisations.

6.5 Test Purchase of Sales to Juveniles

6.5.1 Test purchases may be used by the authority to establish whether juveniles are sold goods illegally (only law enforcement officers should be attempting such transactions for the sale of drugs or stolen items).

6.5.2 When a young person, pursuant to an arrangement with an officer of a public authority, carries out a test purchase at a shop, he is unlikely to

be construed as a CHIS on a single transaction but this would change if the juvenile revisits the same establishment in a way that encourages familiarity.

6.5.3 If covert recording equipment is worn by the test purchaser, or an adult is observing the test purchase, an authorisation for directed surveillance must be obtained and such authorisation must identify the premises involved. In all cases a prior risk assessment is essential in relation to a young person.

6.5.3 When conducting covert test purchase operations at more than one establishment, premises may be combined into a single authorisation provided that each is identified at the outset and the intelligence is sufficient to prevent 'fishing trips'. Necessity, proportionality and collateral intrusion must be addressed in relation to each of the premises. It is unlikely that authorisations will be considered proportionate without demonstration that overt methods have been attempted and failed.

6.6 Mobile Hidden Recording Devices or CCTV

6.6.1 If these devices are to be used to record what is going on in a shop or premises, this will require authorisation as it is directed surveillance.

6.6.2 Where an operation involves both the use of a CHIS and directed surveillance, separate authorisations must be documented and approved in accordance with this Policy.

6.7 Anti-Social Behaviour

Persons who complain about anti-social behaviour and are asked to keep a diary of the incidents that occur will not normally be a CHIS. This is because they are not being asked to establish or maintain a relationship for covert purposes.

6.8 Noise Recording

Recording noise e.g. decibel levels, does not normally record private information and therefore does not require authorisation. Especially sensitive recording devices might be capable of intrusive surveillance, and there is a limit to how long after any notice is served whereby recordings can be said to be made overtly.

7.0 Joint / 3rd Party Investigations and Use of ADC Equipment

7.1 Where the Council undertakes joint surveillance operations, or allows its equipment to be utilised by outside agencies such as the Police, copies of these authorisations must be obtained and placed on the central file.

7.2 The same criteria for the use of covert surveillance and covert human

intelligence sources apply in relation to joint investigations or equipment usage. It is therefore vital that the relevant Officers who undertake external liaison are fully aware of the requirements of RIPA when involved in decisions in relation to joint investigations or the proposed use of the Council's equipment for surveillance purposes.

7.3 Where the Council is requested to take action based upon evidence obtained by a 3rd party under the provisions of RIPA (e.g. licencing action requested by the Police), copies of these authorisations must be obtained and placed on the central file.

8.0 Acquisition of Communications Data

8.1 The Investigatory Powers Act 2016 now covers the powers granted in respect of the acquisition of communications data from telecommunications and postal companies, which the Act terms Telecommunications Operators (TO's) – formerly known as Communication Service Providers (CSP's) under RIPA. The only basis upon which the Council can request this data is for the purpose of preventing or detecting crime or of preventing disorder.

8.2 From November 2018, the Investigatory Powers Act 2016 places further restrictions and local authorities may only acquire event (traffic or service) data where the crime can be defined as a serious crime; otherwise only subscriber data may be obtained. Serious crime means:-

- an offence for which an adult is capable of being sentenced to one year or more in prison;
- an offence committed by a body corporate
- any offence involving violence, resulting in a substantial financial gain or involving conduct by a large group of persons in pursuit of a common goal;
- any offence which involves the sending of a communication or breach of privacy; or
- an offence which involves, as an integral part of it, the sending of a communication or a breach of a person's privacy.

8.3 In the event an application for communications data is required, the National Anti-Fraud Network (NAFN) will be consulted to ensure that the correct form(s) are completed and that the required information is provided, in accordance with the process in sections 8.4-8.5 below.

8.4 Acquisition of communications data under the Act involves the following roles within a relevant public authority:-

- the applicant
- the Approved Rank ('made aware') officer
- the single point of contact
- the senior responsible officer.

8.4.1 The applicant is a person involved in conducting an investigation or operation for a relevant public authority who makes an application for

the acquisition of communications data. The applicant completes an application, setting out for consideration by the Approved Rank officer, the necessity and proportionality of a specific requirement for acquiring communications data.

8.4.2 The Approved Rank ('made aware') officer is a person holding a prescribed office (Service Manager or above) in a relevant public authority who considers the application to confirm that it is necessary and proportionate in the specific circumstances. (For ADC, the list of such officers is contained in Appendix E).

8.4.3 The single point of contact (SPoC) is either an accredited individual or a group of accredited individuals trained to facilitate lawful acquisition of communications data and effective co-operation between a public authority and TO's. To become accredited an individual must complete a course of training appropriate for the role of a SPoC and have been issued a SPoC Personal Identification Number (PIN). Details of all accredited individuals are available to TO's for authentication purposes. (For local authorities including ADC, this role must be undertaken externally by the NAFN SPoC service, who will liaise with the Approved Rank officer to ensure that any requests are appropriate and meet current legal requirements).

8.4.4 Within every relevant public authority a senior responsible officer must be responsible for the integrity of the process in place within the public authority to acquire communications data, compliance with the Act and Code of Practice. (Within ADC, this role is undertaken by the Group Head of Council Advice & Monitoring).

8.4.5 It should be noted that it is now a criminal offence under S11 of the Act if an applicant inappropriately requests data in a 'wilful or reckless' manner.

8.5 NAFN has a published procedure for Councils to request communications data:-

- access to the NAFN system will be required for the applicant to enter the request using the on-line forms provided
- the Approved Rank officer will also require access to the NAFN system to confirm that they have been 'made aware' of the request, that it is necessary and proportionate and in line with the legislation
- the SPoC (NAFN) will consider the request and may require clarification or re-work by the Council
- if NAFN agree the request is appropriate, they will forward it to the Office for Communications Data Authorisations (OCDA) for authorisation (there is no longer a need for Magistrate approval for such requests)
- the OCDA can approve the request, reject it or pass it back for re-work / re-submission via NAFN

- if approved, NAFN will make the request to the Telecommunications Operator and provide the data to the Council once received.

9.0 Duties and Responsibilities of the Authorising Officer

9.1 Officers who are able to give RIPA authorisations will be of a sufficiently senior level within the Council and will have received appropriate training to do so. These Authorised Officers will be named within the Council's published policy at Appendix E.

9.2 The Authorising Officer must not be directly engaged in the investigation and cannot be responsible for authorising investigations into their own activities.

9.3 The Authorising Officer shall not grant authorisation for the carrying out of any activity governed by RIPA unless they believe it is necessary and proportionate.

9.4 Necessity

9.4.1 The action is necessary for one of the reasons specified in Act. The Council is only authorised to use RIPA, subject to the additional restrictions applied by the protection of Freedoms Act 2012 (see section 2.7.4 above):--

- for the purpose of preventing or detecting crime – directed surveillance under Section 28(3)(b) of the Act
- for the purpose of preventing or detecting crime or of preventing disorder – use of a CHIS under Section 29(3)(b) or the Act or the acquisition of communications data under Section 22(2)(b) of the Act.

9.5 Collateral Intrusion

9.5.1 Before authorising surveillance, the Authorising Officer should also take into account the risk of intrusion into the privacy of persons other than those who are directly subjects of the investigation or operation. Measures should be taken, wherever practicable, to avoid or minimise unnecessary intrusion into the lives of those not directly connected with the investigation or operation.

9.5.2 An application for an authorisation should include an assessment of the risk of any collateral intrusion. The Authorising Officer should take this into account when considering the proportionality of the surveillance.

9.5.3 Any person granting or applying for an authorisation will also need to be aware of particular sensitivities in the local community where the surveillance is taking place.

9.6 Proportionality

9.6.1 The authorised surveillance must be proportionate to what the investigating officer is seeking to achieve. Do not use a sledgehammer to crack a nut. The following elements of proportionality should therefore be considered:-

i. balancing the size and scope of the proposed activity against the gravity and extent of the perceived crime or offence;
ii. explaining how and why the methods to be adopted will cause the least possible intrusion on the subject and others;
iii. 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;
iv. evidencing, as far as reasonably practicable, what other methods had been considered and why they were not implemented.

9.7 Reasons for Authorisation

9.7.1 As detailed in Sections 2.7.4 and 9.4.1 above, from 1 November 2012 local authorities can only authorise RIPA use in respect of criminal offences that are punishable by a maximum term of at least 6 months' imprisonment or are related to the underage sale of alcohol or tobacco. This may be required:-

i. in the context of enforcement actions such as prosecutions and appropriate legal proceedings, such as injunctions, possession proceedings and Anti-Social Behaviour Orders (e.g. relating to Housing Benefit fraud, harassment of tenants, breach of Planning regulations, licensing, environmental legislation)
ii. for operations involving test purchases
iii. in the context of personnel matters where the nature of the activity e.g. theft or fraud, is expected to lead to future legal proceedings. (Where the matter would be of a purely disciplinary nature, rather than criminal where the 6 month tariff would be applicable, RIPA would not apply and normal business processes to gather information would be justified).

9.7.2 The Authorising Officer should ensure that there is justification as to why surveillance is necessary and what has been done so far to obtain the information. RIPA authorisation should not be seen as an alternative to attempting other methods of obtaining the information.

9.8 Insurance and Health & Safety

9.8.1 A risk assessment will be required prior to an authorisation for the use of a CHIS or a juvenile (e.g. for test purchases) and it is good practice to do so for other RIPA activity, to ensure compliance with the Health & Safety at Work Act 1974.

9.9 Authorising Officer's Reasoning

9.9.1 It is important that the Authorising Officer records their thought

processes and comments on why they are authorising or refusing the request.

9.10 Time Limits and Reviews

9.10.1 The Act provides that authorisations are for 3 months for Directed Surveillance and 12 months for a CHIS. If it is expected an operation will be completed quickly then a review should be held so that authorisation can be cancelled at the earliest opportunity.

9.11 Authorisation Flowchart

9.11.1 A flowchart in Appendix B sets out the steps an Authorising Officer must take in dealing with a request for authorisation.

10.0 Duties and Responsibilities of Officers Seeking Authorisation

10.1 It is important to be able to distinguish between Directed and Non-Directed Surveillance.

10.1.1 Directed examples are:-

- town centre CCTV to track an individual when the individual is unaware and where this is pre-planned use of the CCTV system for this purpose
- monitoring of individuals to ascertain if they are living together for benefit fraud.

10.1.2 Non-Directed examples are:-

- general observation activities, where the surveillance is not of particular individuals and the intention is to identify and tackle offenders on a reactive basis e.g. standing on a street corner to monitor private hire vehicles plying for hire illegally
- CCTV overt or incidental surveillance
- overt investigations, where a Benefit Officer undertakes a home visit to make enquiries.

10.1.3 Surveillance equipment can be installed, or a CHIS used, for a legitimate purpose only where sufficient evidence exists and has been documented to warrant the exercise, and it can be demonstrated that surveillance is the least intrusive means of meeting that purpose and proportionate to what you are seeking to achieve.

10.1.4 You must ensure you have thoroughly examined all the reasonable alternatives, such as overt surveillance, interview, changing your method of working or security. You must record in writing your considerations and why you have concluded that RIPA authorisation is required. Your application must be made in writing unless it is an

oral authorisation. It must be submitted to an appropriate Authorising Officer (see Appendix E).

10.1.5 Written authorisations for covert surveillance will be valid for 3 months from the date the authorisation is approved by a Magistrate, but will be subject to review within that period to establish whether the authorisation should continue for the entire period.

10.1.6 You should ensure that when considering carrying out covert surveillance it is carefully planned so that the necessary consultations regarding risk assessments, insurance and Health & Safety, availability of officers and equipment can be carried out.

10.2 Operational Considerations - Data Protection

10.2.1 During a covert operation, recorded material or information collected should be stored and transported securely.

10.2.2 Relevant details of the RIPA operation and outcome must be recorded on the appropriate forms covering review, renewal and / or cancellation. This should:-

- record the date and times (if at all) that surveillance took place and the order to cease the activity was made
- the reason for cancellation
- ensure that surveillance equipment has been removed and returned
- provide directions for the management of the product
- ensure that detail of property interfered with, or persons subjected to surveillance, is properly recorded
- record the value of the surveillance or interference (i.e. whether the objectives as set in the authorisation were met).

10.2.3 The Home Office Code of Practice requires that Authorising officers, through their relevant Data Controller, must ensure compliance with the appropriate data protection requirements under the Data Protection Act 2018 and any relevant internal arrangements produced by individual authorities relating to the handling and storage of material. This will cover the dissemination, copying, storage and destruction of private information obtained by the Council.

10.2.4 Under the General Data Protection Regulation / Data Protection Act 2018, evidence should only be retained for as long as necessary and access to it will be restricted to those Officers concerned with the investigation and enforcement.

10.2.5 The Authorising Officer, in consultation with the Council's Group Head of Council Advice & Monitoring, decides whether to allow requests for access to the information by third parties, including Council Officers. Dissemination and/or copying of information obtained should be kept to a minimum.

10.2.6 Access will normally be allowed to prescribed parties, including law enforcement agencies, prosecution agencies, legal representatives and those individuals subject to the surveillance (unless disclosure would prejudice any criminal enquiries or proceedings).

10.3 Equipment

10.3.1 Officers involved in any investigation under RIPA must ensure that equipment used for the gathering of evidence (e.g. CCTV, digital cameras) is of a suitable quality for such evidence to be admissible in Court and that it is collected and secured in accordance with PACE requirements.

10.3.2 Surveillance equipment should be stored securely, with limited access rights, and an inventory held. A deployment record should also be maintained of any use in covert activities and these records will be subject to audit / inspection.

10.4 Criminal or Disciplinary Matters

10.4.1 Once a covert operation results in confirmation of an individual under surveillance as having committed a criminal or disciplinary offence, that individual must be informed of this as promptly as is reasonably practicable, in order to ensure their right to a fair trial or hearing within a reasonable time in accordance with the Human Rights Act.

10.4.2 In a situation where it is considered that a matter gives rise to a potential criminal offence, any interview with the suspect must be carried out under caution and conducted by a suitably trained Officer, or where appropriate the Police must be involved immediately to ensure that evidential procedures and the requirements of current legislation are observed i.e. Police and Criminal Evidence Act 1984 (PACE).

10.4.3 Officers should seek advice from the Legal Services section on these issues if they are unsure as to how to proceed.

10.4.4 Under no circumstances should any covert surveillance operation be given backdated authorisation after it has commenced.

10.5 Authorisation Flowchart

10.5.1 A flowchart in Appendix A sets out the steps an Officer seeking authorisation must take.

11.0 Sources Under 16 and 18 Years of Age

11.1 The RIPA (Juveniles) Order 2000 prohibits the authorisation for the conduct or use of a source if:

(a) the source is under the age of 16; and

(b) the relationship to which the conduct or use would relate is

between the source and his / her parent or any person who has parental responsibility for him / her.

11.2 Where a source is under 16 the arrangements referred to in Section 29 (2)(c) of the Act must be such that there is at all times a person holding an office, rank or position who has responsibility for ensuring that an appropriate adult is present at meetings to which this applies. This applies to all meetings between any person representing the investigating authority and the source, while the source remains under the age of 16.

11.2.1 An appropriate adult is defined as:-

(a) the parent or guardian of the source;

(b) any other person who has for the time being assumed responsibility for his / her welfare; or

(c) where no person falling within paragraph (a) or (b) is available, any responsible person aged 18 or over who is neither a member of nor employed by any relevant investigating authority.

11.3 Authorisation of the Source

11.3.1 Only the Chief Executive (or a designated Director, acting as the Head of Paid Service in his absence) can act as the Authorising Officer where the source is a juvenile.

11.3.2 Any authorisation may not be granted where the source is under 18 at the time of authorisation unless:-

i. the Authorising Officer has made a risk assessment, and in the case of a renewal updated the risk assessment; sufficient to demonstrate;

ii. the nature and magnitude of the risk of physical injury to the source arising out of the conduct detailed in the authorisation;

iii. the nature and magnitude of any risk of psychological distress to the source as a result of carrying out the authorised conduct has been identified and evaluated.

11.3.3 The Authorising Officer must have considered the risk assessment and satisfy himself that any risk identified has been properly explained to and understood by the source.

11.3.4 The Authorising Officer must decide whether the relationship to which the conduct or use would relate is between the source and relative, guardian or person who for the time being has assumed parental responsibility for the source's welfare, and has given particular consideration to whether the authorisation is justified in light of the facts.

11.4 Duration of the Authorisation

11.4.1 The authorisation of the use of a source under the age of eighteen at the time of authorisation or renewal will be for one month only.

12.0 Judicial Approval

12.1 From 1 November 2012, the Protection of Freedoms Act requires that approval of local authority authorisations under RIPA must be obtained from a Justice of the Peace. Authorisations and notices can only be given effect once an order approving the use has been granted by a JP. This will also apply to renewals of existing authorisations.

12.2 The new judicial approval mechanism is in addition to the existing authorisation processes under the relevant parts of RIPA. The flowchart at Appendix C outlines the procedure for applying for judicial approval. The application must be made by the authority that has granted the authorisation.

12.2.1 Following approval by the Authorising Officer / Designated Person, the first stage of the process is for the local authority to contact Her Majesty's Courts and Tribunals Service (HMCTS) administration team at the magistrates' court to arrange a hearing.

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

12.2.3 The original RIPA authorisation or notice should be shown to the JP but will be retained by the local authority so that it is available for inspection by the Commissioners' offices and in the event of any legal challenge or investigation.

12.2.4 In addition, the local authority will provide the JP with a partially completed judicial application / order form:-

- for directed surveillance / CHIS, this form is held on the Council's SharePoint under Internal Audit / RIPA
- for the acquisition of communications data, information must be provided to NAFN (the Council's SPoC) via the Internal Audit Manager and the form downloaded from their system, as part of a Court Pack.

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

12.2.6 For the acquisition of communications data, a copy of the signed judicial application / order form must also be supplied to NAFN to provide them with the necessary authorisation to proceed on the Council's behalf.

12.3 Arranging a Hearing

12.3.1 HMCTS will be the first point of contact for the local authority when seeking a JP approval. The local authority will inform HMCTS administration as soon as possible to request a hearing.

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

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

12.3.4 The Council's Legal Services area will be able to provide the necessary contact information / advice on the relevant Magistrates' Court / HMCTS administration area.

12.4 Attending a Hearing

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

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

12.4.3 Local authorities will want to consider who is best able to answer the JP's questions on the policy and practice of conducting covert operations and detail of the case itself. It is envisaged that the Authorising Officer or case investigator will be able to fulfil this role. They will know the most about the investigation and will have determined that use of a covert technique is required in order to progress a particular case. The local authority may consider it appropriate for the SPoC to attend for applications in respect of communications data. (This does not, however, remove or reduce in any way the duty of the Authorising Officer to determine whether the tests of necessity and proportionality have been met and for considering the appropriate forms and supporting case papers).

12.4.4 The Council's Constitution will designate certain officers who are able to appear and attend at a Magistrate' Court on behalf of the Council under Section 223 of the Local Government Act 1972 and will therefore be able to present RIPA cases to JP's.

12.4.5 Although it is not envisaged that legally trained personnel will be required to make the case to the JP, the Council's Legal Services section will responsible for maintaining the Council's Constitution to ensure that there is an appropriate pool of Officers available to attend a hearing and to provide legal advice and support, as required.

12.5 Decision

12.5.1 The JP will consider whether he or she is satisfied that there are reasonable grounds for believing that the authorisation or notice is necessary and proportionate. They must also be satisfied that the person granting the authority within the Council is appropriate and that it has been made in accordance with applicable legislation.

12.5.2 **The forms and supporting papers must by themselves make the case. It is not sufficient for the local authority to provide oral evidence where this is not reflected or supported in the papers provided**, although the JP may receive and note additional / clarifying information received in the course of the hearing.

12.5.3 If more information is required to determine whether the authorisation or notice has met the tests then the JP will refuse the authorisation.

12.5.4 The JP will record his / her decision on the order section of the judicial application / order form. HMCTS will retain a copy of the local authority RIPA authorisation or notice and the judicial application / order form.

12.6 Outcomes

12.6.1 The JP may decide to:-

- Approve the grant or renewal of an authorisation or notice:-
  - the grant or renewal will then take effect and the local authority may proceed to use the technique in that particular case
  - for communications data, the local authority will be responsible for providing a copy of the of the order to the SPoC
- Refuse to approve the grant or renewal of an authorisation or notice:-
  - the RIPA authorisation or notice will not take effect and the local authority may not use the technique in that case.
  - the local authority may wish to consider the reasons for a refusal (e.g. a technical error in the form which may be remedied without going through an internal authorisation process again) and reapply for judicial approval once this has been rectified
- Refuse to approve the grant or renewal and quash the authorisation or notice:-
  - the court must not exercise its power to quash the authorisation or notice unless the applicant has had at least 2 business days from the date of the refusal to make representations.

13.0 <u>Maintenance of Records of Authorisations, Renewals, Cancellations and</u>

Notices

13.1 The following documents must be retained by the Internal Audit Manager on a central file:-

i. a copy of any authorisation form, together with any supporting documents

ii. a copy of any review and renewal forms, together with any supporting documents

iii. a copy of any cancellation form together, with any supporting documents

iv. a copy of any notice or authorisation in respect of communications data

v. (from 1 November 2012) for any authorisation or renewal a copy of the approval from the Magistrate's Court following judicial review.

13.2 Each form will have a Unique Reference Number (URN) which will be issued by the Internal Audit Manager. This includes rejected applications.

13.3 Authorising Officers MUST forward a copy of each form to the Internal Audit Manager within 1 week of the authorisation, review, renewal, cancellation or rejection.

13.4 The Council will retain records when it is necessary to do so. Records will in the first instance be retained for a period of 3 years from the end of an authorisation so that the Investigatory Powers Commissioner's Office can review the Council's policy and procedures, and individuals' authorisations.

14.0 Training Records

14.1 All Officers who are to authorise applications will be provided with appropriate training by the Council. A central record of this training will be maintained by the Internal Audit Manager and this, and the list of Authorising Officers, updated to reflect changes in personnel.

15.0 Internal Review of the use of RIPA

15.1 Within every relevant public authority it is considered good practice for a senior responsible officer to be made responsible for:-

- the integrity of the process in place within the public authority for the management of CHIS;
- compliance with Part II of the Act and with the Codes;
- oversight of the reporting of errors to the relevant oversight Commissioner and the identification of both the cause(s) of errors and the implementation of processes to minimise repetition of errors;
- engagement with the OSC Inspectors when they conduct their inspections, where applicable; and

- where necessary, oversight of the implementation of post-inspection action plans approved by the relevant oversight Commissioner.

15.2 Within local authorities, the senior responsible officer should usually be a member of the corporate leadership team and should be responsible for ensuring that all Authorising Officers are of an appropriate standard in light of any recommendations in the inspection reports prepared by the Investigatory Powers Commissioner's Office. Where an inspection report highlights concerns about the standards of Authorising Officers, this individual will be responsible for ensuring that the concerns are addressed. The responsible officer for Arun District Council is the Internal Audit Manager.

16.0 Member Review of the use of RIPA

16.1 In order to comply with the latest codes of practice issued by the Home Office, a quarterly report on the Council's use of RIPA legislation, including the number of applications authorised and a brief outline of the reasons for authorisation during the last quarter, will be presented to the Audit & Governance Committee. At the end of each municipal year a further report covering the whole year will be presented to the Audit & Governance Committee.

Appendix A

AUTHORISATION FLOWCHART - REQUESTING OFFICER

Prior to Authorisation the Requesting Officer must:-

Refer to the Corporate Policy and Procedure Document

↓

Decide if directed surveillance or a CHIS is required

↓

Assess if authorisation is in accordance with the law

↓

Is it necessary or can it be undertaken overtly

↓

Is it proportionate - “sledgehammer to crack a nut” test

↓

If a less unobtrusive option is available, use that

↓

Authorisation

Prepare and submit an approval form to Authorising Officer

↓

Judicial Approval

In liaison with the Authorising Officer and / or Legal Services, obtain JP approval

After Authorisation / Judicial Approval the Requesting Officer must:-

Review

Undertake periodic progress reviews with the Authorising Officer

↓

Renew

If a renewal is required, complete an appropriate application and submit to Authorising Officer for authorisation and further judicial approval

↓

Cancellation

If the authorisation is not to be renewed or at any time the surveillance becomes unnecessary / the offence being investigated ceases to meet the crime threshold, immediately complete a cancellation form and submit to Authorising Officer

Appendix B

AUTHORISATION FLOWCHART - AUTHORISING OFFICER

Prior to Authorisation the Authorising Officer must:-

Read the Corporate Policy and Procedure Document

↓

Consider in detail whether all options have been considered.

↓

Consider whether the surveillance or a CHIS is necessary and proportionate – consider collateral intrusion and the risk assessment for use of a CHIS or juvenile

↓

Assess if authorisation is in accordance with the law

↓

ONLY authorise if overt or less intrusive option is not appropriate

↓

Judicial Approval

In liaison with the Authorising Officer and / or Legal Services, obtain JP approval

After Authorisation / Judicial Approval the Authorising Officer must:-

Review

Set a review date(s) and undertake periodic progress reviews with the Requesting Officer

↓

Renew

If a renewal is required, authorise an appropriate application progress for further judicial approval

↓

Cancellation

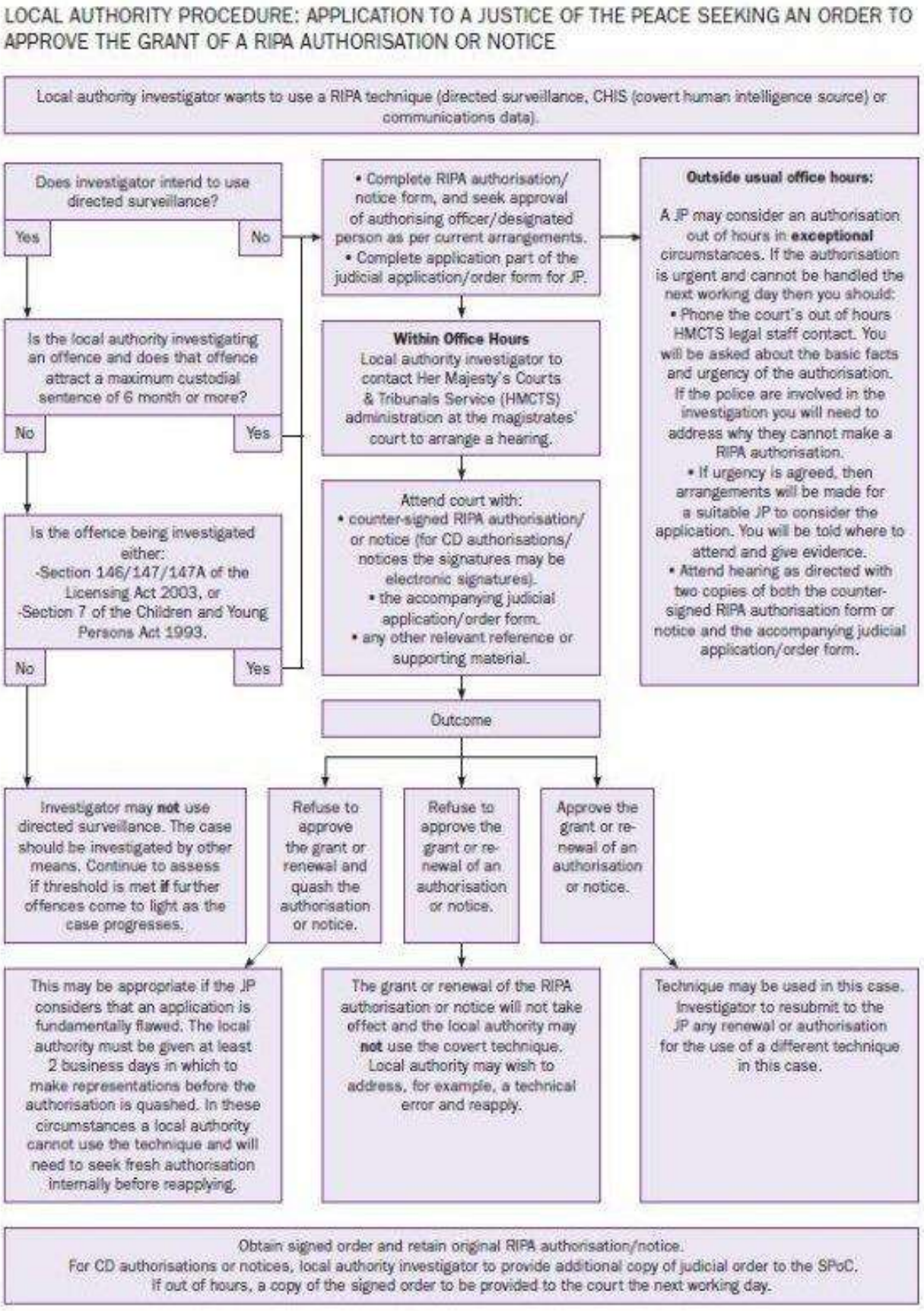
If the authorisation is not to be renewed or at any time the surveillance becomes unnecessary / the offence being investigated ceases to meet the crime threshold, immediately complete a cancellation

↓

Paperwork

Ensure you send all authorisations, renewals, reviews, cancellations, any rejected requests and all relevant judicial approval papers (successful or unsuccessful) to the Internal Audit Manager within 7 days of the relevant event.

Appendix C



Source: 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 D

APPLICATION FORMS

Only approved forms MUST be used. The latest versions of these forms can be found on the Council's SharePoint under Internal Audit / RIPA or in the case of Forms 9 to 11 direct from the Internal Audit Manager

Directed Surveillance

Form 1	Application for Authorisation to Carry Out Directed Surveillance
Form 2	Application for Renewal of a Directed Surveillance Authorisation
Form 3	Review of a Directed Surveillance Authorisation
Form 4	Cancellation of a Directed Surveillance Authorisation

Covert Human Intelligence Source (CHIS)

Form 5	Application for Authorisation of the Conduct or Use of a Covert Human Intelligence Source (CHIS)
Form 6	Application for Renewal of a Covert Human Intelligence Source (CHIS) Authorisation
Form 7	Review of a Covert Human Intelligence Source (CHIS) Authorisation
Form 8	Cancellation of a Covert Human Intelligence Source (CHIS) Authorisation

Acquisition of Communications Data

Form 9	Application for Communications Data
Form 10	Authorisation Under Section 22 (3) Requiring Communications Data to be Obtained and Disclosed
Form 11	Notice Under Section 22 (4) Requiring Communications Data to be Obtained and Disclosed

Judicial Approval

Application for judicial approval for authorisation to obtain or disclose communications data, to use a covert human intelligence source or to conduct directed surveillance

Appendix E

In view of the significance of the restrictions / requirements for judicial approval of RIPA use contained in the Protection of Freedoms Act 2012, the members of the Council's Corporate Management Team will act as Authorising Officers for future RIPA applications:-

AUTHORISING OFFICERS

Chief Executive (Head of Paid Service)	Nigel Lynn
Director of Services	Philippa Dart
Director of Place	Karl Roberts

All authorisations of Covert Human Intelligence Source (CHIS) and Juvenile and Vulnerable Individuals MUST be authorised by the Chief Executive (or a designated Director, acting as the Head of Paid Service in his absence). Likewise any authorisations in respect of investigations into members of staff must be undertaken by the Group Head of Corporate Support or in his absence the Chief Executive.

Similarly, for communications data under IPA only designated officers are registered with NAFN as Approved Rank ('made aware') officers:-

APPROVED RANK OFFICERS

Chief Executive (Head of Paid Service)	Nigel Lynn
Director of Services	Philippa Dart
Director of Place	Karl Roberts
Group Head of Council Advice & Monitoring Officer	Liz Futcher
Internal Audit Manager	Stephen Pearse

Note:-

- The Group Head of Council Advice & Monitoring and / or the Legal Services Manager will provide legal advice and review officer authorisations, as appropriate.
- The Internal Audit Manager will maintain the central register and policy, monitor compliance with the Council's RIPA / IPA processes and provide the appropriate oversight reports required for the Council's Audit & Governance Committee.