Rushmoor Borough Council

THE REGULATION OF INVESTIGATORY POWERS ACT 2000 (RIPA)

CORPORATE POLICY AND PROCEDURES

CONTENTS

1. OVERVIEW

All Officers who carry out (or commission) investigations of any type in the course of their work need to be aware of strict legal requirements that may apply to what they wish to do. All must ensure that they understand and, where necessary comply with, the regulatory framework explained in this document. Refresher training will be organised regularly.

The Senior Responsible Officer (SRO) under this policy (see para 1.2 below) is the Solicitor to the Council, Ann Greaves, who together with the RIPA Coordinator in Legal Services (Diane Milton), oversees compliance with the policy and procedures within the Council. Anyone considering carrying out any investigative activity that may potentially be covered by any of the procedures referred to MUST contact the SRO or the RIPA Coordinator for advice and assistance before undertaking any activity. Specific forms need to be used and procedures followed.

Compliance with RIPA requirements is subject to regular external inspection by the Office of Surveillance Commissioners (the OSC) when all RIPA records are scrutinised by a High Court Judge and officers may be interviewed and asked to account for actions undertaken.

RIPA procedures apply not only to Council officers but also to any other external agency working on the Council's behalf, who would need to obtain authorisation from an authorising officer and the approval of the court before activity could begin.

Particular care needs to be taken when considering using social media as a source of information about an individual, as it is easy to stray into territory where a RIPA authorisation becomes necessary.

The benefit of obtaining RIPA authorisation is that evidence obtained will be lawful, so avoiding successful claims for compensation. This should be borne in mind particularly when considering borderline cases.

There is plenty of material to help officers. In addition to help from Legal Services, current forms, codes of practice and other guidance can be found on Inform.

1.1 Summary

The Regulation of Investigatory Powers Act 2000 ('RIPA') brought into force the regulation of covert investigation by a number of bodies, including local authorities. RIPA regulates a number of investigative procedures, the most recent of which is the access to communications data. This document is intended to provide officers with guidance on the use of covert surveillance, including use of social networking and auction websites, Covert Human Intelligence Sources ('CHIS') and the obtaining and disclosure of communications data under RIPA.

It should be noted that these powers can only be used by officers of the council for the purpose of **preventing or detecting crime (or in the case of a CHIS or obtaining communications data, the further purpose of preventing disorder)**.

Officers must take into account the Codes of Practice issued by the Home Office under RIPA. (See Appendix 4) Further guidance can also be found in the Procedures and Guidance issued by the OSC.

The latest Code of Practice for Covert Surveillance (December 2014) also covers interference with property or with wireless telegraphy as governed by Part III of the

Police Act 1997. It should be noted that Council officers are **not** permitted to undertake this type of activity.

1.2 Background

The Human Rights Act 1998 requires the Council, and organisations working on its behalf, pursuant to Article 8 of the European Convention, to respect the private and family life of citizens, their home and correspondence. The European Convention did not, however, make this an absolute right, but a qualified right. Accordingly, in certain circumstances, the Council may interfere in the citizens' rights mentioned above, if such interference is:

(a) in accordance with the law
(b) necessary (as defined in this document); and
(c) proportionate (as defined in this document)

RIPA provides a statutory mechanism for authorising certain types of surveillance. It seeks to ensure that any interference with an individual's right under Article 8 of the European Convention is necessary and proportionate. In doing so, RIPA seeks to ensure both the public interest and the human rights of individuals are suitably balanced.

If the correct procedures are not followed, evidence may be disallowed by the courts, a complaint of maladministration could be made to the Ombudsman, and/or the Council could be ordered to pay compensation. It is essential, therefore, that all involved with RIPA comply with this document and any further corporate guidance that may be issued from time to time.

Each officer of the Council with responsibilities for the conduct of investigations, must, before carrying out any investigation involving RIPA, undertake appropriate training to ensure that investigations and operations that he/she carries out will be conducted lawfully.

A **Senior Responsible Officer** will be appointed for the Council to ensure the integrity of the process within the Council and its compliance with RIPA, to have oversight of reporting of errors to the relevant oversight commissioner, responsibility for engagement with the OSC when they conduct their inspections and where necessary, oversight of the implementation of any post-inspection action plan. The Senior Responsible Officer will also ensure that Members regularly review the Council's use of RIPA.

1.3 Review

RIPA and this document are important for the effective and efficient operation of the Council's actions with regard to surveillance. This document will, therefore be kept under yearly review by the Senior Responsible Officer and the outcomes of this review will be presented to the Licensing and General Purposes Committee.

Authorising Officers (See para 8 and Appendix 1) must bring any suggestions for continuous improvement of this document to the attention of the Senior Responsible Officer at the earliest possible opportunity.

1.4 Scope

RIPA covers the authorisation of directed surveillance, the authorisation of CHIS sources and the authorisation of obtaining communications data.

Communications data includes information relating to the use of a postal service or telecommunications system but does not include the contents of the communication itself, contents of e-mails or interaction with websites. However, covert targeted monitoring of an individual's activities on a website such as Facebook or Ebay falls under the definition of directed surveillance.

An authorisation under RIPA will provide lawful authority for the investigating officer to carry out surveillance. Failing to obtain authority will not make the surveillance unlawful but could leave the Council open to a civil claim for damages if the person(s) concerned were to seek redress for breach of their Human Rights. If this were to occur, a useful insurance policy (ie RIPA authorisation) would have been discarded.

RIPA forms should be used where **relevant** and they will only be relevant where the **criteria** listed on the forms are fully met.

In terms of monitoring e-mails and internet usage, it is important to recognise the interplay and overlaps with the Council's e-mail and internet policies and guidance (Appendices A and B of the Acceptable Use of IT Policy in the Staff Handbook on Inform), the Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000 and the Data Protection Act 1998.

1.5 Advice

Any officer who is unsure whether what he / she wishes to do would fall within RIPA should refer to the RIPA coordinator in Legal Services.

2. GENERAL

2.1 Definition of Surveillance

'Surveillance' includes:

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

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

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

Surveillance also includes the interception of postal and telephone communications where the sender or recipient consents to the reading of or listening to or recording of the communication. This is a form of directed surveillance.

2.2 Confidential Material

Particular care should be taken in cases where the subject of the investigation or operation might reasonably expect a high degree of privacy, or where confidential information is involved. Confidential information consists of matters subject to legal privilege, confidential personal information, confidential journalistic material and communications between an MP and a constituent.

Applications in which the surveillance is likely to result in the acquisition of confidential material will only be considered in exceptional and compelling circumstances with full regard to the proportionality issues this raises.

The Authorising Officer must give the fullest consideration to any cases where the subject of the surveillance might reasonably expect a high degree of privacy, for instance in his or her home.

Where a likely consequence of surveillance would result in the acquisition of confidential material, the investigating officer must seek authority from the Chief Executive, or, in his absence, the acting Chief Executive.

The use or conduct of a covert human intelligence source (see para 6) to obtain matters subject to legal privilege cannot be undertaken without the prior **approval of the Surveillance Commissioner**.

3. DIRECTED AND INTRUSIVE SURVEILLANCE

3.1 Directed Surveillance

Directed surveillance is surveillance which is covert, but not intrusive (see para 3.2), and undertaken:

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

(b) 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

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

3.2 Intrusive Surveillance

Covert surveillance is intrusive if it:

(a) is carried out in relation to anything taking place on any residential premises or in any private vehicle and

(b) involves the presence of an individual on the premises or in the vehicle or is carried out by means of a surveillance device

Therefore covert surveillance becomes intrusive surveillance if it is carried out involving anything that occurs:

- on residential premises or any private vehicle and
    - involves the presence of someone on the premises or in the vehicle, or
    - is carried out by means of a surveillance device;

Directed surveillance that is carried out in places ordinarily used for legal consultation, at a time when they are being used for such consultations is also treated as intrusive.

With covert surveillance relating to residential premises or private vehicles, if any device used is not on the premises or in the vehicle, it is only intrusive surveillance if

it consistently produces information of the same quality as if it were. This may include eg a camera or a sound recording device.

Where surveillance is carried out by a device designed or adapted principally for the purpose of providing information about the location of a vehicle, the activity is directed surveillance.

Surveillance of commercial premises (such as such as shops) and commercial vehicles (such as taxis) is therefore not intrusive surveillance. The front garden or driveway of premises that are readily visible to the public would not be regarded as residential.

The definition of intrusive surveillance relates to the location of the surveillance and not to a consideration of whether private information is likely to be obtained.

Currently, local authorities are not authorised to carry out intrusive surveillance.

4. IDENTIFYING DIRECTED SURVEILLANCE

Ask yourself the following questions, or follow the flowchart attached as Appendix 2:

4.1 Is the surveillance covert?

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

If your activities are not hidden from the subjects of your investigation, you are not within the RIPA framework at all. In many cases, officers will be behaving in the same way as a normal member of the public (e.g. in the case of most test purchases), and/or will be going about Council business openly (e.g. a market inspector walking through markets).

Similarly, surveillance will be overt if the subject has been told it will happen e.g. where a noisemaker is warned (preferably in writing) that noise will be recorded if the noise continues, or where a licence is issued subject to conditions, and the licensee is told that officers may visit without notice or identifying themselves to the owner/proprietor to check that conditions are being met.

Officers should note that if the same outcome can be achieved by overt means then those means need to be fully explored in the first instance. Covert surveillance must only be undertaken when there is no less invasive way of achieving the outcome.

4.2 Is the surveillance for the purposes of a specific investigation or a specific operation?

Although, the provisions of the Act do not normally cover the use of overt CCTV surveillance systems or Automated Number Plate Recognition (ANPR) in car parks, (since members of the public are aware that such systems are in use), there may be occasions when public authorities use overt CCTV systems and/or ANPR for the purposes of a specific investigation or operation. For example, if the CCTV cameras are targeting a particular known offender. In such cases, authorisation for directed surveillance may be necessary.

4.3 Is the surveillance in such a manner that is likely to result in the obtaining of private information about a person?

Private information includes any information relating to a person's private or family life. The concept of private information should be broadly interpreted to include an individual's private or personal relationship with others. It includes an individual's business and family relationships. Family life itself should be treated as extending beyond the formal relationships created by marriage.

4.4 Is the surveillance otherwise than by way of an immediate response to events or circumstances where it is not reasonably practicable to get authorisation?

Directed surveillance does not include covert surveillance carried out by way of an immediate response to events or circumstances which, by their very nature, could not have been foreseen. For example, a police officer would not require an authorisation to conceal himself and observe a suspicious person that he came across in the course of a patrol.

However, if as a result of that immediate response, you undertake a specific investigation you will need authorisation.

5. INTERNET SITE MONITORING

Access to social network sites is restricted by IT to those whose specific job role requires it and who have obtained written authorisation to access it. (See the Council's corporate policy on the Acceptable Use of IT). The application form for accessing social media sites is found on Inform. Personal use of social network sites is not allowed in work time.

Investigations using social networking sites on the internet such as Facebook, Netlog, Bebo and Myspace, or other open source sites such as Ebay, will fall into the definition of directed covert surveillance if:

(a) The site is not being accessed by the Councils "corporate" registration but by using an individual account aimed at hiding the identity or presence of the investigator and

(b) The site is being used to regularly monitor and record a person's activities, contents of postings or relationships, and

(c) The monitoring is likely to identify private information about the person and/or third parties.

If this is the case then a directed surveillance RIPA authorisation must be obtained which assesses the level of intrusion on the subject and the third parties they are interacting with, balanced against the seriousness of the investigation and potential benefit to the investigation of the activity being conducted.

If the nature of the activity involves establishing or maintaining any form of relationship with the subject, their colleagues or friends with a view to obtaining information, then this activity by a Council employee or someone acting on their behalf, requires authorisation to use a covert human intelligence source (CHIS).

Use of a false identity for covert purposes is permissible if a RIPA authorisation is given.

However, Council employees or someone acting on their behalf must not adopt the identity of a person known, or likely to be known, to the subject of interest or users of the site without

(a) RIPA authorisation,

(b) the explicit consent of the person whose identity is to be used and

(c) giving consideration to the protection of the person whose identity is to be used.

Any investigation of personal social media sites or internet sites beyond open source material may stray into RIPA territory and advice from Legal Services should be sought in advance.

Where privacy settings are available but not applied, data can be regarded as open source, but it should be borne in mind that repeated viewing of open source material may amount to directed surveillance.

6. COVERT HUMAN INTELLIGENCE SOURCES (CHIS)

6.1 Definition

A person is a source if:

(a) they establish or maintain a personal or other relationship with a person for the covert purpose of facilitating the doing of anything falling within paragraph (b) or (c);
(b) they covertly use such a relationship to obtain information or to provide access to any information to another person; or
(c) they covertly disclose information obtained by the use of such a relationship or as a consequence of the existence of such a relationship.

A source may include those referred to as agents, informants and officers working undercover.

A purpose is covert, in relation to the establishment or maintenance of a personal or other relationship, if and only if, the relationship is conducted in a manner that is calculated to ensure that one of the parties to the relationship is unaware of the purpose.

A relationship is used covertly, and information obtained is disclosed covertly, if and only if it is used or disclosed in a manner that is calculated to ensure that one of the parties to the relationship is unaware of the use or disclosure in question.

The use of a source involves inducing, asking or assisting a person to engage in the conduct of a source, or to obtain information by means of the conduct of such a source.

This covers the use of professional witnesses to obtain information and evidence. For example, it will include a professional witness retained by the Council to pose as a tenant to obtain information and evidence against alleged nuisance perpetrators.

Whilst it is unlikely to arise in a local authority investigation, the use or conduct of a source to obtain knowledge of matters subject to legal privilege cannot be undertaken without the **prior approval of the Surveillance Commissioner**.

Carrying out test purchases will not require the purchaser to establish a relationship with the supplier with the covert purpose of obtaining information and, therefore, the purchaser will not normally be a CHIS. For example, authorisation would not normally be required for test purchases carried out in the ordinary course of business (e.g. walking into a shop and purchasing a product over the counter). By contrast, developing a relationship with a person in the shop, to obtain information about the seller's suppliers of an illegal product will require authorisation as a CHIS. Similarly, using mobile hidden recording devices or CCTV cameras to record what is going on in the shop will require authorisation as directed surveillance.

The Home Office Covert Human Intelligence Source Code of Practice (December 2014) (see Appendix 4) states that the provisions of RIPA are not intended to apply in circumstances where members of the public volunteer information to the police or other authorities, as part of their normal civic duties, or to contact numbers set up to receive information (such as Crimestoppers, Customs Confidential, the Anti Terrorist Hotline, or the Security Service Public Telephone Number). Members of the public acting in this way would not generally be regarded as sources.

However, a member of the public may in reality be a CHIS if they provide information covertly obtained in the course of, or as a result of, a personal or other relationship. If this information is acted on, a duty of care would be owed if they were at risk of reprisals. The consideration is the manner in which the information has been obtained (i.e. as a result of a relationship established or maintained for a covert purpose), not whether the informant has been tasked to obtain information for the Council.

An authorisation under RIPA will provide lawful authority for the use of a source.

6.2 Security and Welfare

Only the Chief Executive or, in his absence, the acting Chief Executive, is able to authorise the use of vulnerable individuals and juvenile sources (under 18s).

The Chief Executive must have regard to the special safeguards and provisions that apply to vulnerable individuals and juvenile sources, more particularly set out in the current CHIS Code of Practice.

As a CHIS may be used in difficult or dangerous situations, RIPA requires arrangements to be in place to ensure the security and welfare of the CHIS. The Authorising Officer must ensure that arrangements are in place for the proper oversight and management of sources, including appointing the following individual officers for each source:

A "**Handler**" who will have day-to-day responsibility for:

- dealing with the CHIS on behalf of the Council;
- 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 will usually be of a position below that of the Authorising Officer.

A "**Controller**" who will be responsible for the management and supervision of the "handler" and general oversight of the use of the CHIS.

Officers using a source shall consider the safety and welfare of that source (even after cancellation of the authorisation), and the foreseeable consequences to others of the tasks they are asked to carry out. The Authorising Officer must carry out a risk assessment before authorising the source.

7. COMMUNICATIONS DATA

7.1 Definition

This covers any conduct in relation to a postal service or telecommunications system for obtaining communications data and the disclosure to any person of such data. For these purposes, communications data includes information relating to the use of a postal service or telecommunications system but does not include the contents of the communication itself, content of emails or interaction with websites.

Communications data includes subscribers' details, names and addresses and telephone numbers of those contacted, billing addresses, account information, web addresses visited etc. Two types of data (Customer Data or Service Data) are available to local authorities and, when making an application for obtaining or disclosing such data, the applicant must specify exactly which type of information is required from within each of the subscriber data and service use data sources.

(a) Part C - Customer data – (Subscriber data, RIPA s21(4)(c))

Customer data is the most basic. It is data about users of communication services.

This data includes:

- Name of subscriber
- Addresses for billing, delivery, installation
- Contact telephone number(s)
- Abstract personal records provided by the subscriber (e.g. demographic information)
- Subscribers' account information – bill payment arrangements, including bank, credit/debit card details
- Other services the customer subscribes to.

(b) Part B - Service data – (Service Use data, RIPA s21(4)(b))

This relates to the use of the service provider's services by the customer, and includes:

- The periods during which the customer used the service(s)
- Information about the provision and use of forwarding and re-direction services by postal and telecommunications service providers
- 'Activity', including itemised records of telephone calls (numbers called), internet connections, dates and times/duration of calls, text messages sent
- Information about the connection, disconnection and reconnection of services
- Information about the provision of conference calling, call messaging, call waiting and call barring telecommunications services

- Records of postal items, such as records of registered, recorded or special delivery postal items, records of parcel consignment, delivery and collection
- 'Top-up' details for prepay mobile phones – credit/debit card, voucher/e-top up details

A third type of data (part A - traffic data) defined in RIPA s21 (6) is <u>not</u> accessible to local authorities. This is data that is or has been comprised in or attached to a communication for the purpose of transmitting the communication.

8. AUTHORISATION PROCEDURE

8.1 General

Authorisation is required for the use of directed surveillance, for the conduct and use of sources and for conduct in relation to a postal service or telecommunication system and the disclosure to any person of such data, collectively referred to as the "RIPA powers".

Any officer who undertakes investigations on behalf of the Council (referred to as an Applicant in Appendix 1), must seek <u>provisiona</u>l authorisation in writing from an Authorising Officer in relation to any directed surveillance or for the conduct and use of any CHIS.

Each provisional authorisation then needs to receive judicial approval **before being acted upon.**

The Council`s list of current officers who undertake investigations and so would be considered the case investigating officers are listed in Appendix 1.

It will normally be these officers who will attend the Magistrates' Court for the purpose of presenting RIPA cases to Justices of the Peace (JP) as they will be best placed to answer any questions or clarify any points the JPs have on the application. However, the Authorising Officer's considerations should always be clearly and fully recorded on the application form, and in unusual and complex cases consideration should be given to the Authorising Officer attending the court as well.

Any officer wishing to engage in conduct in relation to a postal service and telecommunication system for obtaining communications data and the disclosure to any person of such data must seek authorisation via NAFN – see the procedure outlined in paragraph 8.6.

Authorising Officers must ensure that staff who report to them follow this policy and do not undertake or carry out any form of surveillance without first obtaining the relevant authorisations in compliance with this policy.

When provisionally authorising surveillance, Authorising Officers must ensure that they clearly set out what activity and equipment has been authorised in order that those conducting the surveillance are clear on what has been sanctioned. The Authorising Officer must fully understand the capability and sensitivity levels of technical equipment that is to be used, and how and where it is to be deployed.

8.2 Who can give Provisional Authorisations?

The 'Authorising Officer' for local authority purposes is any Director, Head of Service, service manager or equivalent. The Council's Authorising Officers are listed in Appendix 1. This appendix will be kept up to date by the Senior Responsible Officer as needs require. The Senior Responsible Officer has the delegated authority to add, delete or substitute names.

An Authorising Officer may grant a provisional authorisation but it does not take effect until it receives judicial approval (See paragraph 9.0).

Please note that certain provisional authorisations, namely those relating to confidential information, vulnerable individuals and juvenile sources, can **only** be granted by the Chief Executive, or, in his absence, the acting Chief Executive.

It will be the responsibility of Authorising Officers who have been formally appointed to ensure their relevant members of staff are also suitably trained as 'applicants' so as to avoid common mistakes appearing on forms for RIPA authorisations.

Training will be given, or approved by the Senior Responsible Officer, before Authorising Officers are allowed to sign any RIPA forms.

8.3 Grounds for Authorisation – the 'necessary & proportionate' test

An Authorising Officer must comply with a number of obligations under the Act before using any of the RIPA powers.

The Authorising Officer must not grant a provisional authorisation for the use of the RIPA powers unless he/she believes:

(a) that a provisional authorisation is necessary and
(b) the provisionally authorised investigation is proportionate to what is sought to be achieved by carrying it out

For local authority investigations, provisional authorisation for surveillance is deemed "**necessary**" in the circumstances of the particular case if it is for the purpose of the **prevention or detection of crime(s) punishable by 6 months' imprisonment or more**, or relates to the sale of alcohol or tobacco to underage persons, and if that objective could not be achieved without the information sought.

It is slightly different for authorising a CHIS where deployment may be "necessary" if it is for the purpose of **preventing or detecting crime or preventing disorder.** (This test was unaffected by the changes introduced by the Protection of Freedoms Act which removed the purpose of preventing disorder in the case of directed surveillance.)

Conduct is not deemed "**proportionate**" in the pursuance of the legitimate aims listed above and will not justify the interference, if the means used to achieve the aim are excessive in the circumstances. Any conduct must meet the objective in question and must not be arbitrary or unfair nor must the impact on any individuals or group be too severe.

The conduct must also be the least invasive method of achieving the end and the risk of intrusion into the privacy of persons other than those who are directly the subjects of the investigation must be assessed and taken into account (see Collateral Intrusion below).

Consideration must be given to the seriousness of the potential offence and whether it could be punishable on summary conviction or on indictment, by a maximum term of at least six months' imprisonment (surveillance authorisations).

Careful consideration needs to be made by Authorising Officers of all these points using the list below:

(a) is the size and scope of the operation balanced by the gravity and extent of the perceived crime or offence?

(b) is it clear how and why the methods to be adopted will cause the least possible intrusion on the subject and others?

(c) is the activity an appropriate use of the legislation and the only reasonable way, having considered all alternatives, of obtaining the necessary result?

(d) has evidence been provided of other methods considered and why they were not implemented?

Such consideration needs to be demonstrated on the authorisation form in the relevant parts. Authorising Officers must exercise their minds every time they are asked to sign a form. They must never sign or rubber stamp the form without thinking about their personal and the Council's responsibilities. Any boxes not needed on the form/s must be clearly marked as being 'not applicable' or a line put through the same. Great care must also be taken to ensure accurate information is used and inserted in the correct boxes. Reasons for any refusal of an application must also be kept on the form and retained for future audits.

So far as possible, Authorising Officers should not be responsible for authorising investigations or operations in which they are directly involved.

8.4 Collateral Intrusion

Before provisionally authorising investigative procedures, the Authorising Officer must also take into account the risk of intrusion into the privacy of persons other than those who are directly the subjects of the investigation or operation (collateral intrusion). The investigating officer must take measures, wherever practicable, to avoid or minimise unnecessary intrusion into the lives of those not directly connected with the investigation or operation; eg it should be made clear where the information will be stored and what will happen to it at the end of the case.

An application for a provisional authorisation must include an assessment of the risk of any collateral intrusion. The Authorising Officer shall take this into account, when considering the proportionality of the use of the RIPA powers.

Where an operation unexpectedly interferes with the privacy of individuals who were not the subject of the investigation or covered by the authorisation in some other way, the investigating officer should inform the Authorising Officer.

9.0 COURT PROCEDURES

9.1 Judicial Approval of Provisional Authorisations and Renewals

The judicial approval mechanism is in addition to the existing authorisation process under the relevant parts of RIPA as outlined in the Codes of Practice. The current local authority process of assessing necessity and proportionality, completing the RIPA authorisation / application form and seeking approval from an authorising officer will remain the same.

The Council is only able to grant a “provisional” authorisation or renewal to make use of any of the RIPA powers. All provisional authorisations and renewals must be approved by the Magistrates’ Court before the use of the RIPA power in the investigation commences.

The Authorising Officer must apply to the local Magistrates’ Court for judicial approval of an authorisation or a renewal of an authorisation. There is no need to give notice of the application to the person(s) subject to the application or their legal representatives. The Authorising Officer will attend the hearing which will take place in private before a single JP. If the Magistrates’ Court refuses to approve the application, it may also make an order quashing the provisional authorisation.

The Authorising Officer will provide the court with a copy of the original RIPA provisional 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 the information that is relied upon**.

The Authorising Officer will also provide a partially completed judicial application form containing a brief summary of the circumstances of the case. This is supplementary to and does not replace the need to supply the provisionally authorised RIPA authorisation or renewal as well.

The JP will consider the provisionally authorised application or renewal, and will need to be satisfied that:

a) At the time of provisional authorisation, there were reasonable grounds for believing that the tests of necessity and proportionality were satisfied in relation to the authorisation, and that those grounds still exist;

b) That the person who granted provisional authorisation was an appropriately designated person; (officers will need to provide a copy of the authorisation).

c) The provisional grant or renewal of any authorisation or notice was not in breach of any restrictions imposed under RIPA; and

d) Any other conditions provided for by an order made by the Secretary of State were satisfied.

The applicant, with the assistance of the Solicitor to the Council, is responsible for tabling the application IN WRITING for judicial approval in the Magistrates’ Court before the use of the RIPA powers commences.

The Home Office has issued guidance to local authorities on the judicial approval process (see Appendix 4).

The order section of the application form will be completed by the JP and will be the official record of the JP`s decision.

Judicial approval is required for all initial RIPA authorisations / applications and renewals and the Council will need to retain a copy of the judicial application order form after it has been signed by the JP. There is no need for the court to consider either cancellations or internal reviews.

The hearing is a 'legal proceeding' and therefore Council officers need to be formally designated to appear and present evidence or provide information as required by the JP. Authorising officers will fulfil the role of applicants.

See paragraph 13 for details of the records to be kept.

9.2 Special Procedure for Communications Data

The Acquisition and Disclosure of Communications Data Code of Practice (See Appendix 4) removed the ability of the accredited Council Officer (Ian Harrison) to directly approach telecommunication service providers to obtain data under RIPA.

Applications for the obtaining and disclosure of communications data can now only be made by the officers listed in Appendix 1 and must be made through the National Anti-Fraud Network (NAFN) via their secure website (www.nafn.gov.uk). Provisional authorisation is to be given by a Designated Officer who must always be independent of the investigation. Designated Officers are listed in Appendix 1.

The process map at Appendix 3 gives guidance on the procedure to be followed.

It is the responsibility of the Council to obtain both provisional authorisation and judicial approval of an application before NAFN are requested to obtain the required communications data. NAFN will carry out the Single Point of Contact "SPoC" role which includes:

(a) where appropriate, assessing whether access to the communications data is reasonably practical for the postal or telecommunications operator;

(b) advising applicants and authorising officers on the practicalities of accessing different types of communications data from different postal or telecommunications operators;

(c) providing safeguards for authentication;

(d) assessing the cost and resource implications to both the authorisation and postal or telecommunications operator.

When considering the desirability of obtaining communications data as part of an investigation, officers not authorised to make applications themselves should refer to an authorised applicant officer to make it on their behalf. Authorised applicant officers will discuss all potential applications with a Designated Officer or a NAFN SPoC.

If considered appropriate, the authorised applicant officer will make a formal application via the NAFN website where it will be reviewed by a NAFN SPoC. When satisfied with the application, the SPoC will then forward it to one of the Council's Designated Officers for provisional approval.

If satisfied that the proposed investigation is both necessary and proportionate, the Designated Officer will complete the relevant parts of the application form. The relevant documents will then be generated by NAFN for presentation to the Magistrates' Court.

Following the Court hearing, the applicant must upload the completed Court documents onto the NAFN website. The SPoC will then liaise with the postal / telecommunications company to obtain the information. Data obtained will be provided through the NAFN website.

Communications data, and all copies, extracts and summaries of it must be handled and stored securely. The requirements of the Data Protection Act 1998 and the principles of the Criminal Procedure and Investigations Act 1996 must be strictly followed.

9.3 Urgency

Urgent verbal authorisations are no longer available in relation to the use of the RIPA powers.

9.4 Standard Forms

All authorisations must be in writing.

The forms for seeking use of the RIPA powers are listed in Appendix 4 and can be found in the Staff Handbook on Inform. The authorisation shall be sought using the standard forms current at the relevant time.

(In the case of communications data, applications can only be via NAFN).

10. ACTIVITIES BY OTHER PUBLIC AUTHORITIES

To avoid conflict between the activities of the Council and other public authorities, the investigating officer must make enquiries of other public authorities e.g. the police, to check whether they are carrying out similar activities if the investigator considers that there is such a possibility.

11. JOINT INVESTIGATIONS

When some other agency has been instructed on behalf of the Council to undertake any action under RIPA, this document and the forms in it must be used (as per normal procedure) and the agency advised or kept informed, as necessary, of the various requirements. They must be made aware explicitly what they are authorised to do.

When some other agency (e.g. police, Customs & Excise, Inland Revenue etc):

(a) Wish to use the Council's resources (e.g. CCTV surveillance systems), that agency must follow its own RIPA procedures. Before any officer agrees to allow the Council's resources to be used for the other agency's purposes, he/she must obtain copies of the RIPA authorisation and judicial approval.

(b) Wish to use the Council's premises for their own RIPA activity, the officer should normally co-operate unless there are security or other good operational or managerial reasons as to why the Council's premises should not be used for the agency's activities. In such cases, the Council's own RIPA forms should not be used as the Council is only assisting and not being involved in the RIPA activity of the external agency.

In terms of (a), if the police or other agency wish to use the Council's resources for general observation, as opposed to a specific operation requiring RIPA authorisation, an appropriate letter requesting the proposed use, remit, duration, details of who will be undertaking the general observation and the purpose of it must be obtained from the police or other agency before any Council resources are made available for the proposed use.

12. DURATION, RENEWALS AND CANCELLATION OF AUTHORISATIONS

12.1 Duration

Authorisations must be reviewed in the time stated (whether or not surveillance has begun) and cancelled once no longer needed. Authorisations last for:

(a) 12 months from the date of the judicial approval for the conduct or use of a source (1 month in the case of a juvenile CHIS);

(b) three months less a day from the date of the last judicial approval for directed surveillance;

(c) one month from the date of judicial approval for communications data, or earlier if cancelled under Section 23(8) of the Act.

12.2 Reviews

The Authorising Officer must decide how often to review the authorisation and record it on the application form. He/she must then undertake regular reviews of authorisations to assess the need for the surveillance to continue. As a minimum these should be carried out monthly from the start date.

Applicants should submit a review form by the review date set by the Authorising Officer; any changes in circumstances since the original application should be recorded so that the need to continue the activity can be assessed.

The results of a review should be recorded by the Authorising Officer. If circumstances or techniques to be used have changed significantly, a new authorisation should be sought and submitted to a JP for approval.

Where the surveillance provides access to confidential information or involves collateral intrusion the officer should conduct more frequent reviews.

Standard review forms for directed surveillance and CHIS are in the Staff Handbook on Inform.

12.3 Renewals

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

Authorisations can be renewed in writing at any time up to and including the date of expiry. An authorisation cannot be renewed after it has expired. The Authorising Officer must consider the matter afresh, including taking into account the benefits of the surveillance to date and any collateral intrusion that has occurred. The renewal will begin on the day when the authorisation would have expired provided the necessary judicial approval has been obtained.

A further requirement in relation to renewal of covert human intelligence sources, is that judicial approval will only be granted if the Magistrates are satisfied that a review has been carried out, which considers:

- the use made of the source in the period since authorisation was granted (or the last renewal); and
- the tasks given to the source during that period, and the information obtained from the conduct or use of the source;

and for the purposes of making an Order, the Magistrates have considered the results of that review.

The Authorising Officer who granted or last renewed the authorisation must cancel it if he is satisfied that the investigative procedure no longer meets the criteria upon which it was authorised.

Standard renewal forms for the authorisation of directed surveillance and CHIS can be found in the Staff Handbook on Inform.

12.4 Cancellations

An Authorising / Designated Officer must cancel a notice or authorisation as soon as it is no longer necessary, or the conduct is no longer proportionate to what is sought to be achieved. The duty to cancel falls on the Authorising / Designated Officer.

In the case of a notice issued in respect of communications data, the relevant postal or telecommunications operator must be informed of the cancellation.

Standard cancellation forms for directed surveillance and CHIS can be found in the Staff Handbook on Inform. Cancellations in respect of communications data must be done via the NAFN website.

When completing a cancellation form, care should be taken to record when the activity ceased, what value the surveillance had been to the investigation, what evidence "products" had been obtained and what was to happen to it.

13. RECORDS

The Service Head of a service carrying out investigations must keep a detailed record of all provisional and judicially approved authorisations, reviews, renewals, cancellations and rejections in his/her service.

A Central Register of all such forms will be maintained and contain the following information:

(a) an operational unique reference number (URN) for the authorisation
(b) a reference: this is usually the investigation or operation case reference;
(c) the type of authorisation or notice;
(d) the date the provisional authorisation or notice was given;
(e) name and grade of the Authorising Officer;
(f) whether the investigation or operation is likely to result in obtaining confidential information;
(g) whether the provisional authorisation was granted by an individual directly involved in the investigation;
(h) the date and time that judicial approval was granted or refused;
(i) the dates set for review;
(j) if the authorisation or notice is renewed, when it was provisionally renewed and who authorised the renewal, including the name and grade of the Authorising Officer, and the date and time that judicial approval was obtained;
(k) the date the authorisation or notice was cancelled;
(l) the outcomes of the use of the powers, including any instructions given by the Authorising Officer.

These records must be retained for a period of at least three years from the ending of the authorisation. [1]

13.1 Maintaining the Central Record of all Authorisations

The Senior Responsible Officer will hold and monitor the centrally retrievable record of all provisional and judicially approved authorisations. This is held on Sharepoint and access to it is limited to named / specified officers.

Authorising Officers must pass all relevant information to the Senior Responsible Officer within 1 week of every judicial approval, review, cancellation or rejection, for entry onto the register.

On cancellation, the applicant or Authorising Officer must inform the Senior Responsible Officer of the outcome of the use of the RIPA powers in relation to their investigation.

13.2 Records maintained in Services

The Authorising Officer will maintain the following documentation, which need not form part of the centrally retrievable record:

(a) the original signed application and a copy of the provisional authorisation or notice if applicable together with a copy of any order of judicial approval or refusal, as well as any supplementary documentation and notification given by the Authorising Officer;
(b) a record of the period over which the surveillance has taken place;
(c) the frequency of reviews prescribed by the Authorising Officer;
(d) an original signed record of the result of each review of the authorisation or notice;
(e) the original signed renewal of an authorisation or notice, together with the supporting documentation submitted when the renewal was requested;
(f) the date and time when any instruction was given by the Authorising Officer.

Each form must have an operational URN and Central Register number. The cross-referencing of each URN takes place within the form for audit purposes. Rejected forms will also have URNs.

13.3 Other Records of Covert Human Intelligence Sources

Proper records must be kept by Services of the authorisation and use of a source. An Authorising Officer must not grant a provisional authorisation for the use or conduct of a source unless he/she believes that there are arrangements in place for ensuring that there is at all times a person with the responsibility for maintaining a record of the use made of the source.

The Service records , which are to be kept for at least **five** years shall contain the following information:

(a) the identity of the source;
(b) the identity, where known, used by the source;
(c) any relevant investigating authority other than the Council;
(d) the means by which the source is referred to within each relevant investigating authority;

[1] Source: Covert Surveillance and Property Interference Code of Practice

(e) any other significant information connected with the security and welfare of the source;

(f) any confirmation made by a person granting or renewing an authorisation for the conduct or use of a source that the information in paragraph (d) has been considered and that any identified risks to the security and welfare of the source have where appropriate been properly explained to and understood by the source;

(g) the date when, and the circumstances in which, the source was recruited;

(h) the identities of the persons who, in relation to the source;

i. hold day-to-day responsibility for dealing with the source and for the source's security and welfare

ii. have a general oversight of the use made of the source (not to be the person identified in (h) (i))

iii. have responsibility for maintaining a record of the use made of the source

(i) the periods during which those persons have discharged those responsibilities;

(j) the tasks given to the source and the demands made of him in relation to his activities as a source;

(k) all contacts or communications between the source and a person acting on behalf of any relevant investigating authority;

(l) the information obtained by the conduct or use of the source;

(m) any dissemination of information obtained in that way; and

(n) in the case of a source who is not an undercover operative, every payment, benefit or reward and every offer of a payment, benefit or reward that is made or provided by or on behalf of any relevant investigating authority in respect of the source's activities for the benefit of that or any other relevant investigating authority. [2]

13.4 Checks on the Integrity of the Process

A nominated officer will carry out a regular review to check whether the relevant records have been completed as necessary.

The Senior Responsible Officer will carry out a periodic sample check of all RIPA authorisations, renewals cancellations and rejections.

The Licensing and General Purposes Committee will consider internal reports on the use of the 2000 Act to ensure that it is being used consistently with the local authority's policy and that the policy remains fit for purpose. Changes to the policy will be made by the Cabinet.

14. RETENTION AND DESTRUCTION

Material obtained from properly authorised surveillance or a source may be used in other investigations. Arrangements shall be in place for the handling, storage and destruction of material obtained through the use of covert surveillance, a source or the obtaining or disclosure of communications data. Authorising Officers must ensure compliance with the appropriate data protection requirements and any relevant corporate procedures relating to the handling and storage of material.

[2] Source SI 2000/2725

Where the product of surveillance could be relevant to pending or future proceedings, it should be retained in accordance with established disclosure requirements for a suitable period and subject to review.

15. CONSEQUENCES OF IGNORING RIPA

RIPA states that if authorisation confers entitlement to engage in a certain conduct and the conduct is in accordance with the authorisation, then **it shall be lawful for all purposes.**

Where there is interference with the right to respect for private and family life guaranteed under Article 8 of the European Convention on Human Rights, and where there is no other source of lawful authority, the consequence of not obtaining an authorisation under RIPA may be that the action is unlawful by virtue of section 6 of the Human Rights Act 1998.

Officers must seek an authorisation where the directed surveillance, or the obtaining or disclosure of communications data is likely to interfere with a person's Article 8 rights to privacy by obtaining private information about that person, whether or not that person is the subject of the investigation or operation.

Authorisations for the use of a CHIS do not specifically relate to private information, but to the covert manipulation of a relationship to gain any information. Obtaining an authorisation will ensure that the action is carried out in accordance with law and subject to stringent safeguards against abuse.

16. SCRUTINY OF INVESTIGATORY BODIES

The Office of Surveillance Commissioners (OSC) and Interception of Communications Commissioner's Office (IOCCO) have been established under RIPA to facilitate independent scrutiny of the use of RIPA powers by the investigatory bodies that are subject to it. The OSC will inspect Councils to ensure compliance with RIPA and can audit/review the Council's policies and procedures, and individual authorisations. The IOCCO will inspect NAFN records and procedures.
Further details of the OSC can be found at www.surveillancecommissioners.gov.uk .

The Investigatory Powers Tribunal has been established under RIPA to deal with complaints from members of the public about the use or conduct by public authorities of these powers. The Tribunal is separate from the OSC. The Council expects its officers to co-operate fully with these bodies and to bring forward any proposals for improvement that may follow on from an inspection report or a Tribunal hearing.

IF IN DOUBT ADVICE MUST BE SOUGHT FROM THE SENIOR RESPONSIBLE OFFICER

17 DOCUMENT CONTROL

17.1 Document control:

Organisation	Rushmoor Borough Council
Title	Regulation of Investigatory Powers Act 2000 Policy and Procedures

Author	Diane Milton
Filename	
Owner	Solicitor to the Council
Endorsed by	Cabinet
Review	Every 2 years

17.2 Revision history:

Version	Author	Date	Comments
1	Diane Milton	February 2017	

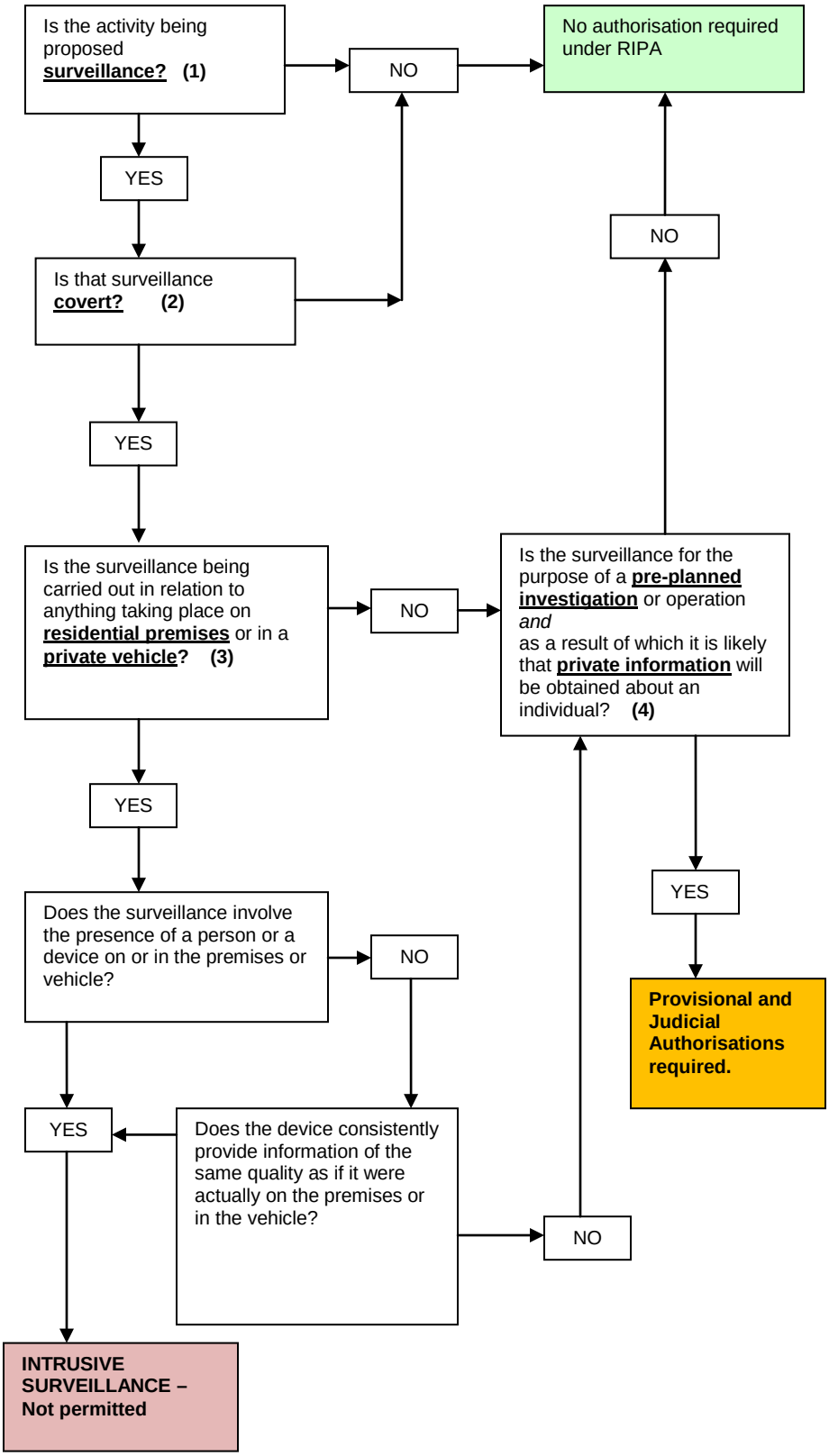
APPENDIX 1

Officer Appointments to Roles in the Policy

Role	Appointed Officer	Tasks
Senior Responsible Officer	Solicitor to the Council	Ensure the integrity of the process within the Council and its compliance with RIPA, including carrying out a periodic sample check of the quality of RIPA authorisations, renewals and cancellations. Carry out an annual review of the corporate policy. Have oversight of the completion of annual returns to the relevant oversight commissioner. Engage with the oversight commissioners when they conduct their inspections and where necessary, oversee the implementation of any post-inspection action plan. Have oversight of reporting of errors to the relevant oversight commissioner Ensure that Members regularly review the Council's use of RIPA.
DIRECTED SURVEILLANCE / COVERT HUMAN INTELLIGENCE SOURCES		
Role	**Appointed Officers**	**Tasks**
Higher level authoriser	Chief Executive or acting Chief Executive in his / her absence	Approve applications involving confidential material (surveillance) or the use of vulnerable individuals and juvenile sources (CHIS)
Authorising Officers (Surveillance/ CHIS)	Chief Executive Audit Manager Environmental Health Managers: 1.Pollution / Environmental control 2. Licensing Head of Financial Services	Review applications for considerations of: • lawfulness • proportionality, • collateral intrusion and provisionally approve or reject them. Carry out risk assessment if use of CHIS being requested Ensure appointment of controller and handler to be responsible for a CHIS Attend Magistrates' Court to obtain judicial approval

COMMUNICATIONS DATA		
Role	**Appointed Officers**	**Tasks**
Designated Officers (Communications Data)	2 Corporate Directors	Assess application following consideration by NAFN SPoC Review lawfulness, necessity, proportionality, collateral intrusion Provisionally authorise or reject **Must be independent of the investigation**

APPENDIX 2
DIRECTED SURVEILLANCE FLOW CHART



(1) Surveillance includes: monitoring, observing, listening to persons, their movements, their conversations or their other activities or communications. It includes recording anything monitored, observed or listened to in the course of surveillance, and surveillance by or with the assistance of a surveillance device

(2) Covert is defined as surveillance which is carried out in a manner calculated to ensure that the person(s) who are subject to it are unaware that it is or may be taking place

(3) Residential premises: occupied or used by a person, however temporarily, for residential purposes or otherwise as living accommodation including hotel rooms – but not communal areas – e.g. a hotel lounge.

Private vehicle: which is used primarily for the private purpose of the owner or a person having the right to use it – but not, e.g. a minicab.

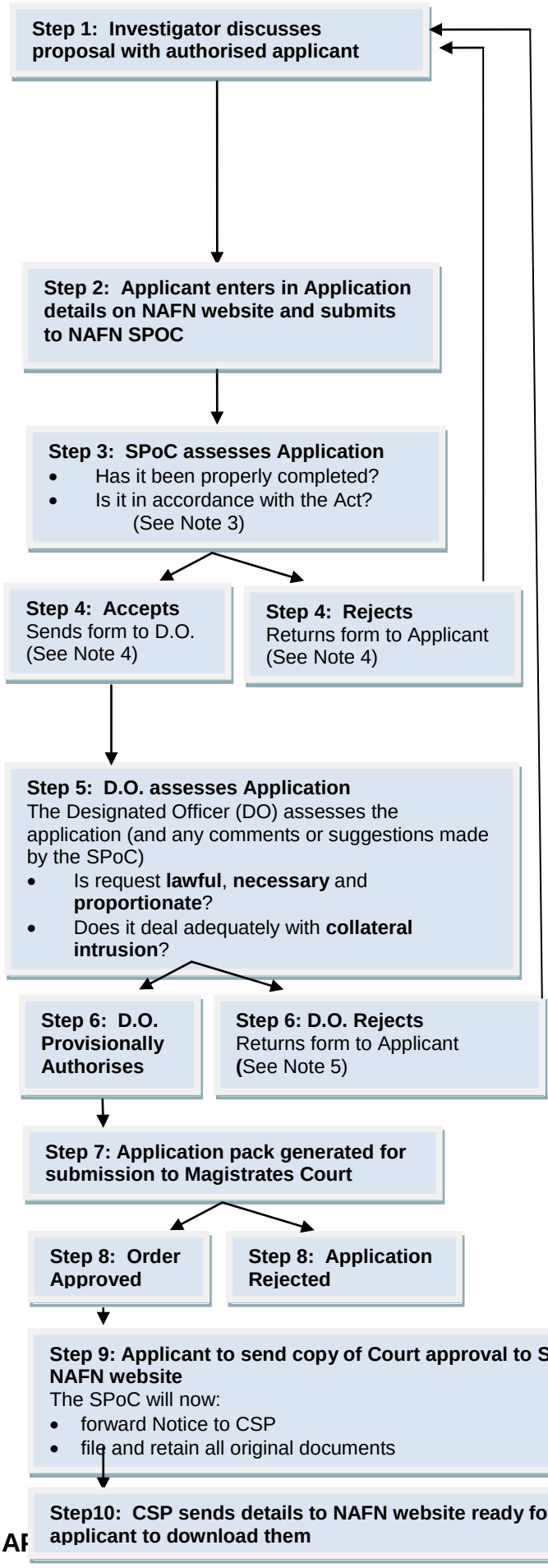
(4) Pre-planned investigation: surveillance is not planned if it is conducted as an immediate response to events or circumstances the nature of which it would not be reasonably practicable for authority to be sought.

Private information: includes any information relating to a person's private or family life. This must be interpreted broadly to include an individual's relationship with others. It will include information about a person's associations, lifestyle, finances etc. It is immaterial whether the person about whom the information will be gathered is the subject of the investigation.

Note: Before provisionally authorising any directed surveillance investigation, the Authorising Officer (AO) must clearly indicate in the authorisation form itself that the AO does believe that the proposed investigation is both **necessary** for preventing or detecting crime **and** that the investigation is **proportionate** to what it is sought to achieve. The AO must also show that any potential **collateral intrusion** has been taken into account and that reasonable steps are proposed to minimise such intrusion.

APPENDIX 3

Flowchart of Application Process for Communications Data



Note 1 The purpose of the discussion is to try to find alternative options for obtaining the information required.

Applicant may also wish to discuss content, scope and aims of the application and type of application with the NAFN SPoC before submitting the application

Note 2 The application should include:

- The purpose for which the data is required
- The nature of the enquiry
- Details of the data required
- The timescale in which the data is needed
- A statement clearly setting out:
  - why request is **necessary**
  - why request is **proportionate**
  - steps to be taken to minimise **collateral intrusion**

Note 3 The SPoC will:

- ensure application is practical and lawful
- advice on most appropriate route
- assess cost and resource implications

Note 4 If the SPoC **accepts** that the application is justified and reasonably practicable, s/he:

- will submit the application to the DO for approval
- include any appropriate additional information/comments for consideration by DO

If the SPoC **rejects** the application, s/he will:

- return the application to the applicant
- specify in writing reason(s) for rejection

Note 5 If D.O. **authorises** the application, s/he will:

- Approve online
- document any discussions conducted in reaching the decision

If D.O. **rejects** the application, s/he will:

- return the application to the applicant
- specify in writing reason(s) for rejection
- save a copy of rejected application + reason(s) and pass to the SRO for entry into the Council's Central Record

KEY

Applicant: *Officer making the application*
D.O.: *Designated Officer who provisionally authorises the Application*
SPoC: *Single Point of Contact between RBC and CSP*
CSP: *Communications Service Provider*

RIPA Forms, Codes of Practice and Guides – see Staff Handbook on Inform for current versions

Directed Surveillance

- Authorisation
- Review
- Renewal
- Cancellation
- Covert Surveillance and Property Interference Code of Practice (Dec 14)

Covert Human Intelligence (CHIS)

- Authorisation
- Review
- Renewal
- Cancellation
- Covert Human Intelligence Sources Code of Practice (Dec 14)

Communications Data

National Anti-Fraud Network - https://secure.nafn.gov.uk/

- Acquisition and Disclosure of Communications Data Code of Practice (Mar 15)

Application for judicial approval - communications data, to use covert human intelligence source or to conduct directed surveillance

- Judicial approval application form
- Draft court order
- The judicial approval process for RIPA and the crime threshold for directed surveillance (Oct 12)

Guidance

- Office of Surveillance Commissioners Procedures and Guidance (Dec 14)

Other

- Application form for access to Social Media sites