APPENDIX A

POLICY & PROCEDURES
on
ACCESSING COMMUNICATIONS DATA
under the
REGULATION OF INVESTIGATORY POWERS ACT 2000
as amended by The Protection of Freedoms Act 2012

Version 3.1
Amended: February 2014

Up to date copies are available on the Source

CONTENTS

NOTE:

This document must be read in conjunction with the Home Office Code of Practice on Accessing Communications Data.

Copies of this document and links to the Code of Practice are located on *the Source*.

The Council's Policy & Procedure on Covert Surveillance & use of Covert Intelligence Sources are contained in a separate document located on *the Source*.

SOUTHWARK COUNCIL POLICY & PROCEDURES ON ACCESSING COMMUNICATIONS DATA UNDER THE REGULATION OF INVESTIGATORY POWERS ACT 2000 (RIPA)

A Background

The Human Rights Act 1998 requires the council, and organisations working on its behalf, to have respect for the private and family life of citizens. However, in rare cases, it may be necessary for the council to act covertly in ways that could interfere with an individual's rights.

The Regulation of Investigatory Powers Act 2000 ('RIPA') provides a mechanism for authorising council staff to access limited information from telecommunications companies. It aims to ensure that any interference with individual's privacy is necessary and proportionate, and that both the public interest and the human rights of individuals are protected. It also provides a mechanism for covert surveillance and the use of a "covert human intelligence source" ('CHIS') - e.g. undercover agents).

It is important to note that the legislation does not just affect directly employed council staff. All external agencies working for southwark council automatically become a public body under the act for the time they are working for the council. It is essential therefore that all external agencies comply with the RIPA too, and that work carried out by agencies on the council's behalf be properly authorised by one of the council's Designated Persons. If the correct procedures are not followed, evidence could be thrown out, a complaint of maladministration could be made to the Ombudsman, the council could be the subject of an adverse report by the Office of the Surveillance Commissioners or the Interception of Communications Commissioner, or a claim could be made leading to the payment of compensation by the council.

Senior Responsible Officer

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 Chapter II of Part I of the Act and with this code, and
- oversight of the reporting of errors to the Commissioner and the identification of both the cause(s) of errors and the implementation of processes to minimise repetition of reported errors.

The council's Senior Responsible Officer is its Monitoring Officer, Doreen Forrester-Brown, Head of legal services. The Monitoring Officer's nominee is Norman Coombe. The Senior Responsible Officer is therefore responsible for this policy and any queries should be referred to Norman Coombe.

B Changes to the RIPA process

The Protection of Freedoms Act 2012 came into force on 1 November 2012 and requires that the acquisition of communications data should be subject to a magistrates approval mechanism. Section 37 of the PFA 2012 amended RIPA by inserting two new sections (23A and 23B). These sections require judicial approval from a magistrate after the grant by a "relevant person" of an authorisation or notice to obtain communications data. A relevant person is defined in the new section 23A(6) as an individual holding an office, rank or position in a local authority.

C Accessing Communications Data

1 General

Chapter II, Part 1 of RIPA is concerned with the requisition, provision and handling of communications data, sets out the council's duties and responsibilities, and the system of safeguards that must be followed to ensure we do not breach an individual's rights set out under the European Convention on Human Rights, in particular their right to privacy. The Interception of Communications Commissioner oversees compliance with this part of the Act.

Communications data (CD) is the 'who', 'when' and 'where' of a communication, but not the 'what' (i.e. the content of what was said or written). RIPA groups CD into three types:

- "traffic data" (which includes information about where the communications are made or received);
- "service use information" (such as the type of communication, time sent and its duration); and
- "subscriber information" (which includes billing information such as the name, address and bank details of the subscriber of telephone or internet services).

Access to communications data is most likely to be needed to identify the owner of a particular telephone number or internet address. All requests seeking to obtain communications data must be properly authorised using the procedure set out in this document. Appendix 1 provides a flow chart of the process from application consideration to recording of information to assist officers in complying with this Policy and Procedure.

2 What RIPA does & doesn't do – Communications Data

Under RIPA a local authority can only authorise the acquisition of the less intrusive types of CD: service use and subscriber information.

RIPA does

- allow the council to request limited communications data from telecommunications service providers or a postal service only:
  - in its capacity as a local authority, and
  - where it is necessary for the purposes of preventing or detecting crime or of preventing disorder.
- allow the council to have access to the communications data which:
  - relates to, or in connection with, the use or provision of a Communications Service Provider ("CSP") e.g. telecommunications or postal service, by any person, or
  - any other information held or obtained by the CSP about that person, except traffic data or the contents of the communication.
- allow the council to obtain details of the source and destination of a message, for example through itemised telephone records.

In practice this means that access under these powers is limited to telephone, facsimile, postal and email subscriber and billing information.

RIPA does not:

- allow the council to obtain details of incoming calls or email communications;

- allow the council to obtain the content of the communications;
- allow the council to obtain cellular location data.

Under no circumstances can local authorities be authorised to obtain traffic data under RIPA. Local authorities are not permitted to intercept the content of any person's communications and it is an offence to do so without lawful authority.

Detecting crime includes establishing by whom, for what purpose, by what means and generally in what circumstances any crime was committed, the gathering of evidence for use in any legal proceedings and the apprehension of the person (or persons) by whom any crime was committed. See section 81(5) of RIPA.

3 Categories of data

As a local authority the council is allowed access to obtain the following categories of data under RIPA:

Section 21(4)(b)

Outgoing itemised phone billing;
Outgoing email transmissions;
Information about data uploads and downloads; and
Records of connections to internet services.

Section 21(4)(c)

Subscriber details for a telephone, including ex-directory and mobile numbers (customers' names and addresses);
Subscriber details for an email account;
Subscriber details for a domain name (website address);
Account details including application forms, method of payment; and
Customer contact notes.

The council is **not** allowed access to obtain the following category of data:

Section 21(4)(a)

cellular location data (traffic data); nor
details of incoming calls or email communications.

It *may* be possible to obtain the above category of data with the involvement of the police.

D Authorisations and Notices

RIPA provides two different ways of authorising access to communications data:

(1) through an Authorisation under s22 (3) of RIPA - which allows the council to collect or retrieve the data ourselves; or

(2) by a Notice under s22(4) of RIPA – where a Notice is given to a Communications Service Provider (CSP) to collect or retrieve the data and then provide it to the council.

E Who does what – Applicants, Single Points of Contact (SPoCs) and Designated Persons

1 Applicants

The Applicant is generally the investigating officer who will have primary responsibility for making applications for access to communications data and arranging and attending

magistrates hearings. Only nominated officers in the trading standards, corporate anti-fraud and community safety and enforcement teams may submit an application for access to communications data. Any other officer wishing to make an application must first be approved by the Monitoring Officer (Doreen Forrester-Brown) or her nominated representative (Norman Coombe). All applications must follow the process in this guide.

2 Single Points of Contact (SPoC)

All applications for communications data must be made electronically through the National Anti-Fraud Network (NAFN) who act as the council's ***single point of contact (SPoC***). This is to ensure a centralised and managed approach in making applications to obtain communications data and facilitates lawful acquisition of communications data and effective co-operation between the council and Communication Service Providers (CSPs). The accredited SPoCs at NAFN examine the council's applications independently and provide advice to applicants and Designated Persons to ensure that the council acts in an informed and lawful manner. Any queries regarding the use of NAFN should be referred to Norman Coombe who acts as the council's main point of contact with NAFN.

3 Designated Persons (DPs)

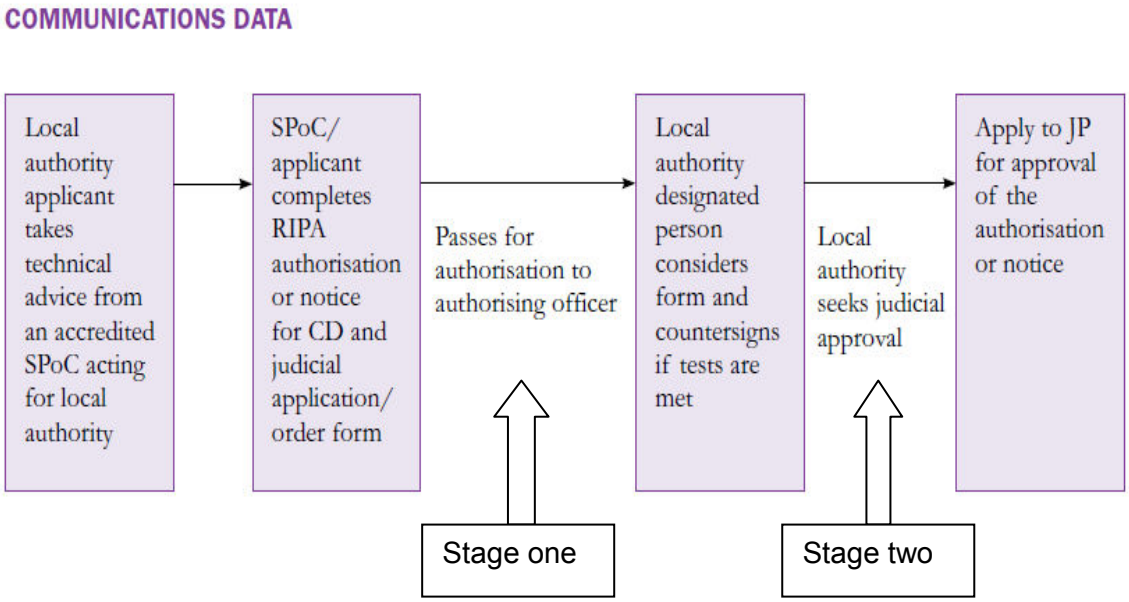
Only a Designated Person may authorise access to communications data. Designated Persons must be a "Director, Head of Service, Service Manager or equivalent" [Regulation of Investigatory Powers (Communications Data) Order 2010].

The council's **Designated Persons** are listed in Appendix 2 and have been notified to NAFN. No other person may authorise an application under any circumstances.

F Applications for Communications data

Communications data may only be accessed if the proper two stage RIPA and approval process is followed:

- Stage one – internal authorisation via the NAFN website
- Stage two – approval by a Magistrate.



A more detailed flowchart is included in Appendix 1.

G Stage One – Internal Authorisation

1 Applicants

All applications for Communications Data must be made using NAFN. The Applicant will need to:

- Register as a user on www.nafn.gov.uk
- Complete and submit the electronic Application Form to NAFN.

The NAFN Application Form is included for reference in Appendix 3. Home Office guidance on how to complete the Application Form – for Applicants and for Designated Persons is available on the Source and on www.nafn.gov.uk.

2 SPoC - The National Anti Fraud Network (NAFN)

NAFN will review the Application Form. If changes need to be made it will be referred back to the Applicant with suggestions, otherwise the NAFN SPoC will complete the relevant part of the Application Form and forward it electronically to a Designated Person for authorisation. When DP authorisation is obtained, NAFN will forward an electronic pack to the Applicant containing the signed Application Form and the signed Magistrates form so that stage two can be commenced.

3 Designated Person

The Designated Person will review the Application Form that has been electronically forwarded to them by NAFN, and complete the appropriate parts of the form with their comments. The form should then be resubmitted electronically to NAFN.

Whilst ideally the Designated Person should not be responsible for authorising their own activities, that is, those operations or investigations in which that officer is directly involved or for which they have direct responsibility, (paragraph 3.1 1 of the Code of Practice) there is some latitude for DPs to approve such applications, even though they have had some direct involvement, as it is recognised that this may be unavoidable in small organisations. In such cases, however, it is a requirement of the Code of Practice that the DP must outline their involvement in the investigation or enquiry and the justification for undertaking the role of the DP must be explicit in the recorded considerations. It is recommended that the council should strive to achieve as much independence in the approvals process as possible.

The Designated Person must be able to justify the decision to authorise the application requesting access to communications data. In order to do this he/she must consider:

- whether, in the case being considered, accessing the communications data is necessary and justified in order to prevent or detect crime or prevent disorder; and

- whether obtaining access to the data is proportionate to what is sought to be achieved, taking account of the scope of the conduct that is required to meet the request, e.g. where accessing the communications data is likely to result in the intrusion into the privacy of a person who is not the focus of the notice, whether the circumstances of the case still justify access to the data.

- that they are satisfied that the request is undertaken in connection with a local authority function and that it is necessary for the purposes of preventing or detecting crime or of preventing disorder.

A Designated Person will make a decision whether to issue a notice based upon the Application that is made. The Application form is not served upon the CSP that holds the

data. The Notice that they receive contains only enough information to allow them to fulfil their duties under RIPA to locate and provide the information.

H Stage two – Approval by a magistrate

1 Applicants

The Applicant will need to:

- submit the application to the magistrates court and arrange the hearing;
- attend the hearing;
- upload a copy of the magistrates order to the NAFN SPoC.

2 Arrange a hearing

The first stage of the process is for the Applicant to contact Her Majesty's Courts and Tribunals Service (HMCTS) administration team at the magistrates' court to arrange a hearing. This will be at the Camberwell Green magistrates court. There should be no fee for this hearing.

3 Documents

The court will need:-

- Sight of the original signed authorisation (plus a copy) and any supporting documents
- A partially completed judicial application order form counter-signed by a Designated Person. (This is provided by NAFN with an electronic signature and has been accepted by the court previously).

These documents MUST by themselves make the case. It is not sufficient for the council to provide oral evidence where this is not reflected or supported in the papers provided. The magistrate may note on the form any additional information he or she has received during the course of the hearing but information fundamental to the case must be included in the authorisation form.

In order to maintain privacy, notice of the application is not required to the person whom the authorisation concerns or that person's legal representatives.

4 Attending a Hearing

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 Magistrate.

The hearing will be in private (not in open court) and no press, public, the subject of the investigation or the subject's legal representative will be present. The application will be heard by a single magistrate who will read and consider the RIPA authorisation or notice and the judicial application/order form. S/he may have questions to clarify points or require additional reassurance on particular matters and therefore the case investigator should attend as they will know the most about the investigation and will have determined that access to communications data is required in order to progress a particular case.

The council's constitution designates chief officers as being able to authorise certain officers for the purpose of presenting RIPA cases to the court under section 223 of the Local Government Act 1972. Chief officers should give such authorisations in writing and make a record of who is authorised.

Where such officers are authorised an officer from legal services is not required to attend the hearing.

5 Decision

The magistrate will consider whether he or she is satisfied that:

- at the time the authorisation was granted or renewed, there were reasonable grounds for believing that the authorisation was necessary and proportionate;
- there continues to be reasonable grounds;
- the person who granted the authorisation was an appropriate designated person within the local authority
- the authorisation was made in accordance with any applicable legal restrictions.

The magistrate may decide to:-

- **Approve the grant or renewal of an authorisation** - The grant or renewal of the RIPA authorisation will then take effect.

- **Refuse to approve the grant or renewal of an authorisation or notice** - The RIPA authorisation will not take effect and the local authority may not use the technique in that case. A technical error in the form may be remedied without going through the internal authorisation process again and the council can then reapply for judicial approval once those steps have been taken. If more information is required to determine whether the authorisation or notice has met the tests then the magistrate will refuse the authorisation and the internal authorisation will need to be amended and re-authorised before being re-submitted to the court.

- **Refuse to approve the grant or renewal and quash the authorisation or notice** This applies where a magistrates' court refuses to approve the grant, giving or renewal of an authorisation or notice and decides to quash the original authorisation or notice. The court must not exercise its power to quash that authorisation or notice unless the applicant has had at least 2 business days from the date of the refusal in which to make representations.

6 Emergency Applications

On the rare occasions where out of hours access to a magistrate is required two partially completed judicial application/order forms must be provided so that one can be retained by the magistrate. The council should provide the court with a copy of the signed judicial application/order form the next working day.

However, in most emergency situations where the police have power to act, then they are able to authorise activity under RIPA without prior magistrate's approval. Where renewals are timetabled to fall outside of court hours, for example during a holiday period, it is the council's responsibility to ensure that the renewal is completed ahead of the deadline. Out of hours procedures are for emergencies and should not be used because a renewal has not been processed in time.

7 SPoC (NAFN)

Upon receipt of the magistrates order from the Applicant authorising the application, the NAFN SPoC will then acquire the CD on behalf of the council generally by way of an

Authorisation which enables them to access the CD directly. Otherwise, NAFN will issue a Notice to the CSP.

I Duration of Notices

Notices will only be valid for a maximum of one month unless renewed.

The period of validity will begin on the date the Notice is approved by the magistrate. This means that the notice should have been served within that month. The Designated Person approving the Notice and/or the magistrate may specify a shorter validity period than one month if a shorter period is sufficient to meet the purposes for making the request. This is one of the issues that must be weighed up in considering the proportionality of the request.

Where the notice requires a CSP to collect the data, the Notice may only require disclosure of the data collected during the month of the notice's validity.

Where the Notice requires a CSP to provide data they already hold, disclosure may only be required of data in the possession of operator at the time the Notice is issued.

J Renewal of Notices

A Notice may be renewed during the period it is valid by following the same procedure as obtaining the original notice i.e. both stage one and stage two need to be completed before the expiry of the original authorisation. A renewed Notice takes effect from the expiry date of the Notice it is renewing. Authorisations may be renewed more than once if it is still considered necessary and proportionate and approved by the magistrate.

Applications for renewals should not be made until shortly before the original authorisation period is due to expire but the council must take account of factors which may delay the renewal process (e.g. weekends, court or officer availability).

NAFN will liaise with a Designated Person if there are any time expiration issues which might require an application to be renewed. However this happens very rarely as the nature of the access requests and the use of the authorisation rather than notice process by NAFN mean that it is unlikely that notices will need to be renewed.

K Cancellation of Notices

A Notice must be cancelled as soon as it is no longer necessary, or proportionate in achieving the aim for which the communications data was sought. NAFN will cancel a Notice within their system where required and will notify the Designated Person and CSP. Magistrates approval is **not** required.

L Disclosures of Data

Once NAFN has acquired the communications data on behalf of the council, NAFN will forward it to the Applicant. This data may only be further disclosed in accordance with the council's obligations under the Data Protection Act 1998 and should be stored securely.

M Record Maintenance

The council must keep a detailed record of all Applications, Notices, Authorisations, Renewals and Cancellations [Paragraphs 6.1 – 6.18 Code of Practice]. NAFN complies with these requirements on the council's behalf.

1 Universal Reference Number for Authorisations

NAFN allocates a Universal Reference Number (URN) for each application – this should be quoted on any correspondence.

2 Monitoring and Reporting

NAFN provide an annual return to the Monitoring Officer (as the Senior Responsible Officer) containing full details of all applications submitted by the council. It is the responsibility of the council to then submit that report to the ICCO annually.

3 Confidentiality

Communications data, and all copies, extracts and summaries of it, must be handled and stored securely in accordance with the DPA.

Departments that make applications for access to communications data should ensure that their records of the application and any subsequent notice/authorisation, should it be granted, are kept confidential. Only those officers involved in the application and approval process should have access to the records.

It is the responsibility of individual departments to ensure that any records they hold relating to applications for access to communications data are held in accordance with this policy and in compliance with RIPA and the DPA.

Applicants must ensure that all electronic information in relation to their applications and data received is stored securely and appropriately and is available for inspection or audit (whether internal or external) upon request.

Officers should not make any unnecessary copies of information obtained as a result of an Application, and all records should be securely destroyed as soon as it is no longer needed for any of the authorised purposes.

The council must hold all records until it has been audited by the Interception of Communications Commissioner.

A record of all applications and notices must be maintained for **seven years**. This should include not only those Applications granted, but also those refused. Once the retention period has expired, records must be destroyed confidentially and securely.

4 Error reporting

NAFN keep a record of any errors that have occurred in the issuing of notices, and a report and explanation is sent by NAFN's Senior Responsible Officer to the Commissioner as soon as is practical (paragraphs 6.9 - 6.22 Code of Practice).

5 Complaints

If a complaint is brought to the Investigatory Powers Tribunal, the Council must retain all records relevant to that complaint until the matter is finalised.

N Oversight, Review and Amendments

1 Oversight Procedures

The Senior Responsible Officer (SRO) shall establish and maintain regular meetings not less than twice a year with the Designated Persons to check and test processes and address any training requirements. The SRO shall arrange an oversight meeting as soon as practicable following an inspection to discuss issues and outcomes as appropriate.

The SRO shall record any issues arising out of authorisation applications, the statutory considerations, reviews and cancellations and shall review the quality of authorisations granted from time to time.

The SRO shall carry out analysis of such issues and shall decide appropriate feedback to the Designated Persons. Such information and conclusions shall also be reported to Standards Committee.

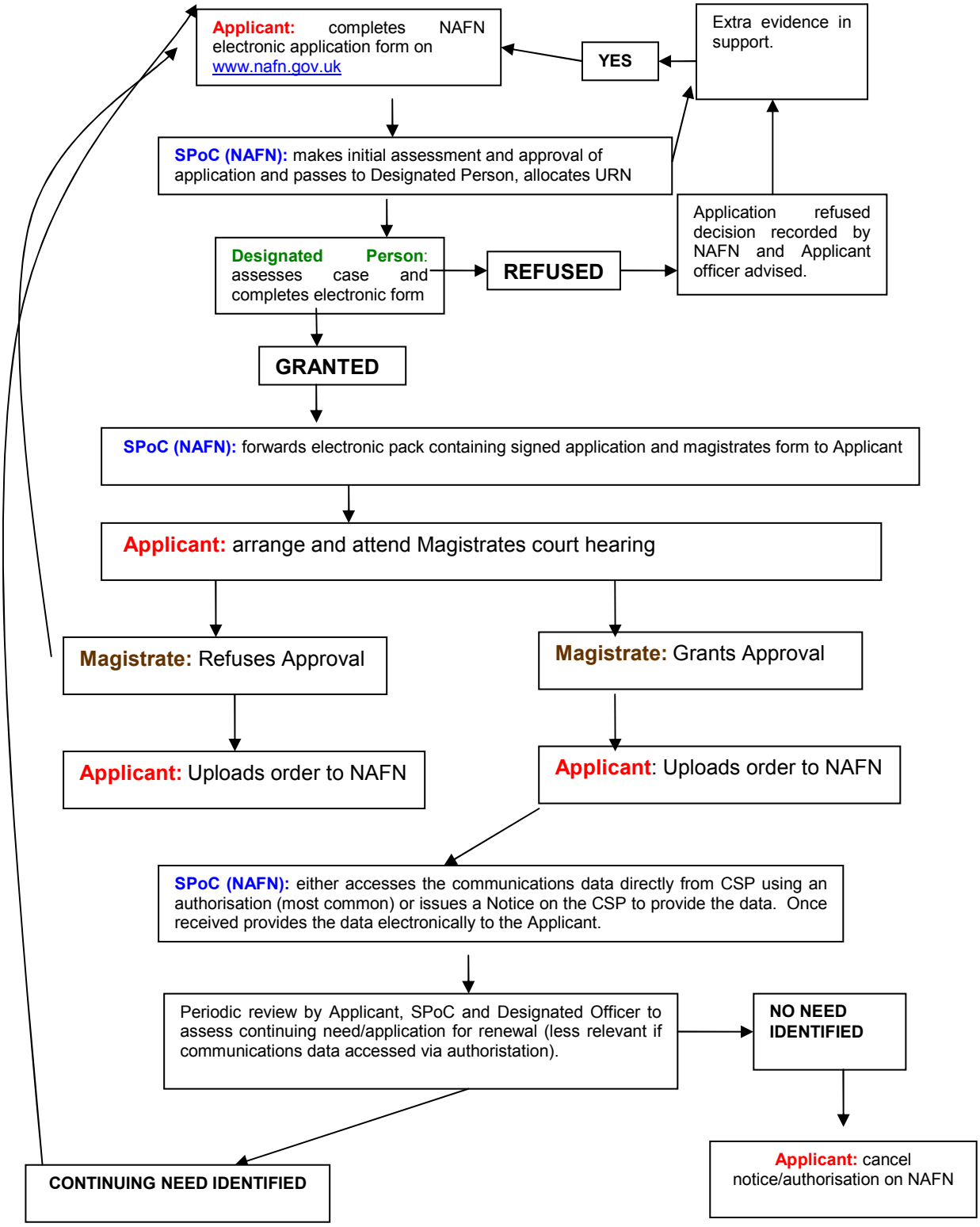
2 Review

This policy will be review every two years and approved by the relevant Cabinet Member. The members of the Standards Committee shall review the use of RIPA 2000 and this policy at least once a year. In order to facilitate this, the SRO shall provide quarterly reports to Standards Committee meetings on how RIPA 2000 has been used in the previous three months and whether there are any concerns as to the policy.

3 Amendments To This Policy And Procedures

The Monitoring Officer is duly authorised to keep this guidance document up to date, and to amend, delete, add or substitute any provisions as s/he deems necessary. For administrative and operational effectiveness, s/he is also authorised to amend the list of Designated Persons set out in Appendix 2, by adding, deleting or substituting any posts.

Appendix 1 Flow Chart of Communications Data Process



Appendix 2 - Designated Persons

The council's Designated Persons are:

Jonathon Toy: Head of Community Safety & Enforcement

Michael Pinder: Head of Anti-Fraud and Internal Audit

Des Waters: Head of Public Realm

These officers are listed as Designated Persons at NAFN and no other officers are authorised to act as a Designated Person under any circumstances. Proposed changes or additions to the list of Designated Persons must be notified to the Monitoring Officer who will, if appropriate, notify those amendments to NAFN.

Appendix 3 - NAFN Application Form

(for information purposes only – all applications must be made online at www.nafn.gov.uk)

NATIONAL ANTI-FRAUD NETWORK

Chapter II of Part I of the Regulation of Investigatory Powers Act 2000

Application for Communications Data

1) Applicant's Name		**4) Unique Reference Number**	
2) Office, Rank or Position		5) Applicant's Telephone Number.	
3) Applicant's Email Address		**6) Applicant's Fax Number**	

7) Operation Name/Reference Number (if applicable)		**8) STATUTORY PURPOSE** **Prevention and detection of crime**

9) COMMUNICATIONS DATA

Describe the communications data required, specifying, where relevant, any historic or future date(s) and, where appropriate, time period(s)

10) NECESSITY

State the nature of the investigation or operation and how it relates to a purpose at question 8

Give a short explanation of the crime (or other purpose), the suspect, victim or witness and the phone or communications address and how all these three link together.

11) PROPORTIONALITY

State why obtaining the communications data is proportionate to what you are seeking to achieve

Outline what is expected to be achieved from obtaining the data and explain how the level of intrusion is justified when taking into consideration the benefit the data will give to the investigation. When considering the benefits to the investigation or operation, can the level of intrusion be justified against the individual's right to privacy? Explain why you have requested the specific date/time periods i.e. how these are proportionate.

12) COLLATERAL INTRUSION

Consider and, where appropriate, describe any meaningful collateral intrusion – the extent to which the privacy of any individual not under investigation may be infringed and why that intrusion is justified in the circumstances

If you have identified any meaningful degree of collateral intrusion, explain what it is.

13) TIMESCALE **Identify and explain the timescale within which the data is required**	

14) APPLICANT **I undertake to inform the SPoC of any change in circumstances that no longer justifies the acquisition of the data**			
Applicant's Signature		**Date**	

15) ASSESSMENT BY ACCREDITED SPoC.	
How much will the acquisition of the data cost?	
Are there other factors the DP should be aware of? *For example, the requirement:* • *is NOT reasonably practical for the CSP to do;* • *will cause an adverse cost or resource implication to either your public authority or the CSP (for instance does the investigation or operation have the analytical capacity to undertake analysis of the communications data once acquired);* • *will produce excess data to that required.*	
Name of Accredited SPoC	

16) AUTHORISATION (Completed by Accredited SPoC when appropriate)

Specify the reason why the collection of communications data by means of an authorisation is appropriate:

☐ There is an agreement in place between the public authority and the CSP relating to the appropriate mechanisms for the disclosure of the data ◇

☐ The designated person considers there is a requirement to identify to whom a service is provided (for example subscriber check) but a CSP has yet to be conclusively determined as the holder of the communications data ♦

☐ CSP is not capable of obtaining or disclosing the communications data Δ

Describe the communications data to be acquired specifying, where relevant, any historic or future date and/or time periods sought. ***Describe the course of conduct required to obtain the data.***	☐ ◇Traffic or Service Use data – acquisition by SPoC directly from CSP ☐ ♦ Subscriber Information – acquisition by SPoC or, where SPoC can not acquire data directly from CSP, serve assurance of the Authorisation on CSP[1] ☐ ΔOther conduct – specify

The statutory purpose for which the conduct may be authorised is set out at section 8 of this form.

The office, rank or position of the designated person should be recorded within section 17 of this form together with a record of the date & time the granting of an authorisation is made.

17. DESIGNATED PERSON

The Designated Person considers the application and if approved records their considerations:

- *Why do you **believe** acquiring the communications data is necessary for one of the purposes within section 22(2) of the Act;*
- *Why do you **believe** the conduct involved in obtaining the data is proportionate to the objective(s)? In making that judgement you should take in consideration any additional information from the SPoC. If the applicant has identified any meaningful degree of collateral intrusion, why you **believe** the request remains justified and proportionate to the objective(s)?*

My considerations in approving / not approving this application are:

[1] See paragraph 3.30 of the code

☐ I authorise the conduct to be undertaken by the SPoC as set out in section 16 of this form. ☐ I give Notice and require the SPoC to serve it on (insert name of CSP) . The Notice bears the unique reference number			
Name		***Office, Rank or Position***	
Signature		**Time and Date**	