POLICY and PROCEDURES
on
THE ACQUISITION AND RETENTION OF COMMUNICATIONS DATA
under the
INVESTIGATORY POWERS ACT 2016

Version 5.0
Amended: August 2022

Up to date copies are available on the Source

CONTENTS

This document must be read in conjunction with the Home Office Communications Code of Practice November 2018 .

Copies of this document and links to the Code of Practice are located on *the Source.* The council's Policy and Procedure on Covert Surveillance and use of Covert Intelligence Sources are contained in a separate document located on *the Source*.

SOUTHWARK COUNCIL POLICY AND PROCEDURES ON THE ACQUISITION AND RETENTION OF COMMUNICATIONS DATA UNDER THE INVESTIGATORY POWERS ACT 2016 (IPA)

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 Investigatory Powers Act 2016 ('IPA') 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 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 IPA too, and that work carried out by agencies on the council's behalf be properly authorised. 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 Investigatory Powers Commissioner (IPC), or a claim could be made leading to the payment of compensation by the council.

B Changes to the Communications Data regime

Relevant sections of the IPA and the Data Retention and Acquisition Regulations 2018 came into force on 31 October 2018 and this amends the legislative scheme providing for the retention of and access to communications data. These changes were required to ensure the UK's communications data regime complies with EU law. The regulations also brought into force the Communications Data Code of Practice (CoP) under the IPA. The amendments to the legislation include:

- A new power for the IPC to authorise communications data requests made by the council. This power has been delegated to a new body – the Office for Communications Data Authorisations (OCDA);
- The acquisition of communications data by local authority officers is no longer subject to judicial approval by a magistrate.
- New terminology for communications data (CD) – Entity Data and Events Data
- Revised statutory purpose for the acquisition of CD – applicable crime purpose
- A new threshold of "serious crime" which includes offences where an adult may be sentenced to imprisonment for at least 12 months and any offence committed by a body corporate for Events Data;
- New offences for unlawful acquisition and disclosure of communications data (s11 and s82)
- Judicial approval required for applications identifying or confirming the identity of a journalist's source
- New option to seek guidance on novel or contentious circumstances
- Public authorities to retain OCDA decision documents
- Reference to Internet Connection Records (LAs not able to acquire these)

C Senior Responsible Officer (CoP 4.10)

Within the council a Senior Responsible Officer must be responsible for:

- the integrity of the process in place within the council to acquire communications data;
- engagement with authorising officers in the Office for Communications Data (OCDA)
- compliance with Part 3 of the IPA and with the Communications Data Code of Practice;
- oversight of the reporting of errors to the IPC and the identification of both the cause(s) of errors and the implementation of processes to minimise repetition of errors;
- ensuring the overall quality of applications submitted to OCDA by the council;
- engagement with IPC inspectors when they conduct their investigations; and
- where necessary, oversight of the implementation of post-inspection action plans approved by the IPC.

The council's Senior Responsible Officer is responsible for this policy and is its Monitoring Officer Doreen Forrester-Brown Director of Law and Governance. The Monitoring Officer's nominee to assist her in administering these procedures is set out in Appendix 2 and any queries on this policy should be referred to them.

D Scope and Definitions (CoP S1)

1 General

Part 3 of the IPA is concerned with the acquisition of communications data and in conjunction with the 2018 regulations and the Code of Practice, 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 Investigatory Powers Commissioner oversees compliance with this part of the Act.

For the purposes of the IPA communications may comprise two broad general categories of data - Systems data and Content. Communications Data is a subset of systems data and is limited to data which does not reveal anything of what might reasonably be considered to be the meaning of the communication.

Communications data (CD) is therefore the 'who', 'when', 'where' and "how" of a communication, but not the 'what' (i.e. the content of what was said or written).

Communications Data can include:

- The way in which, and by what method communications occur;
- The address to which a letter is sent;
- The time and duration of a communication;
- The telephone number or email address of the originator and recipient;
- The location of the device from which the communication was made
- Electronic communications including internet access, internet telephony, instant messaging and the use of applications; and
- Postal services.

Communications Data is generated, held or obtained in the provision, delivery and maintenance of communications services i.e. postal services or telecommunications services.

2 Telecommunications Communications Data (CoP 2.22 – 2.45)

CD comprises four elements:

- Data about an entity to which a telecommunications services is provided and relates to the provision of the service
- Data comprised in, included as part of, attached to or logically associated with a communication for the purposes of a telecommunication system that facilitates the transmission of that communication
- Data which relates of the use of a service or system
- Data which is about the architecture of a telecommunication system

Entity and Events Data – all Communications Data held by a telecommunications operator or obtainable from a telecommunications system falls into two categories:

Entity Data – this data is about entities or links between them and a telecommunication service or system and describes or identifies the entity but does not include information about individual events. Entities can be individuals, groups and objects (such as mobile phones or other communication devices). Examples include subscriber checks, subscriber's account information, connection services, information about devices and preferential numbers.

Events Data – this data identifies or describes events in relation to a telecommunications system which consist of one or more entities engaging in an activity at a specified point, or points, in time. It generally contains more intrusive CD including information on who has been in communication with whom, a person's location when their mobile device connects to the network and internet connection records. Examples include incoming call records, the location of a mobile device, sender or recipient identification information, routing information identifying apparatus, numbers called, service usage information, amounts of data downloads and use of subscribed services such as call waiting.

3 Postal Communications Data (CoP 2.46 –2.53)

CD in relation to a postal service is defined in s262(3) IPA and comprises three elements:

- Postal data which is or has been comprised in or attached to a communication for the purpose of the service by which it is transmitted;
- Data relating to the use made by a person of a postal service;
- Information held or obtained by a postal operator about persons to whom the postal operator provides or has provided a communications services and which relates to the provision of the service.

Examples include information about the subscriber to a PO Box number or a postage paid impression used on bulk mailings, information about the provision to a subscriber or account holder of forwarding/redirection services and subscriber's account information including names and addresses for installation and billing including payment methods and details.

4 Web Browsing and Communications Data (CoP 2.60 – 2.67)

A web address – uniform resource locator (URL) – contains different types of information. The port which is an extended part of the IP address and is required to make the communication process function and the userinfo (where required to route a communication) will be Communications Data. An authorisation under Part 3 of the IPA may only authorise the acquisition of communications data, and therefore can only cover those elements of a URL which constitute communications data.

5 Internet connections records (ICR) (CoP 2.74 – 2.80)

An ICR is a record of an event held by a telecommunications operator about the service to which a customer has connected on the internet. Access to an ICR can enable a public

authority to make further enquiries of an identified social networking provider. Local authorities are prohibited from seeking the processing or disclosure of ICRs for any purpose.

E Communications data acquisition and disclosure

1 General

The acquisition of CD under Part 3 of the IPA will be a justifiable interference with an individual's human rights under Article 8 and, in certain circumstances, Article 10 of the European Convention on Human Rights, only if the conduct being authorised or required to take place is necessary for the purposes of a specific investigation or operation, proportionate and in accordance with law.

Before the council can obtain communications data, authorisation must be given by the Investigatory Powers Commissioner (IPA s60A) in accordance with 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 the IPA does & doesn't allow – Communications Data

Under the IPA the council can only obtain authorisation for the acquisition of communications data where the IPC considers that it is necessary for the council to obtain the data for the **applicable crime purpose** (IPA s61(7)(b).

Events Data

This means that where the communications data is wholly or partly events data for the purpose of preventing or detecting **serious crime** (s86(2A) IPA)**:**

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

Issues commonly investigated by the council, such as fraud, fly tipping, counterfeiting and money laundering are likely to meet the definition of "serious crime".

Entity Data

In relation to Entity Data, this means for the purpose of preventing or detecting crime or of preventing disorder, as the serious crime threshold does not apply.

The council may not make an application that requires the processing or disclosure of internet connection records for any purposes (CoP 8.7).

3 Communications Data involving certain professions (CoP 8.8-8.44)

Communications data is not subject to any form of professional privilege (the fact a communication took place does not disclose what was discussed, considered or advised). However, the degree of interference with an individual's rights and freedom may be higher if they are a member of a profession which handles privileged information – doctors, lawyers, journalists, MPs etc. If an application is to be made for the communications data of those known to be in such professions the application must note this and, at the next inspection, such applications should be marked for the IPC's attention. The applicant must take particular care when making the application including any unintended consequences and whether the public interest is best served. Issues surrounding the infringement of the right to

freedom of expression may arise where a request is made for the communications data of a journalist. The applicant must follow CoP guidance at paragraphs 8.8 – 8.44 and should also notify the Monitoring Officer who will seek advice from the Home Office, the IPC, OCDA and National Anti-Fraud Network as necessary.

Where the purpose of an application is to identify or confirm the identity or role of an individual as a source of journalistic information, Judicial Commissioner approval must be sought (except where there is an imminent threat to life).

4 Novel or contentious application (CoP 8.45-8.54)

The council must take particular care where it is considered that a CD application is novel or contentious, for example, new technical methods of acquisition, new types of CD, unusual sensitivity regarding the nature of the target. Advice on these cases may be sought from the OCDA or a Judicial Commissioner and the advice included in the application.

5 Considerations in relation to the acquisition of internet data

- The council is prohibited from seeking the processing or disclosure of Internet Connection Records for any purpose
- Identifying the sender of an online communication – a request for Internet protocol address resolution (IPAR) should follow the standard authorisation process and the additional steps set out in CoP 9.24.

6 Authorisations (CoP Chapter 6)

The following types of conduct may be authorised:

- Conduct to acquire CD – which may involve the council obtaining CD ourselves or asking any person believed to be in possession of or capable of obtaining the CD to obtain and disclose it; and/or
- The giving of a notice – allowing the council to require by a notice a telecommunications operator to obtain and disclose the required data.

F Who does what – Applicants, Verifying Senior Officers, Single Points of Contact (SPoCs), and the Authorising Individuals), (the OCDA and a Judicial Commissioner)

1 Applicants

The Applicant is generally the investigating officer who will have primary responsibility for making applications for the acquisition of communications data. 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 Senior Responsible Officer (Doreen Forrester-Brown). All applications must follow the process in this guide.

2 Single Points of Contact (SPoCs)

All applications for communications data by the council 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. The accredited SPoCs at NAFN examine the council's applications independently and provide advice to applicants to ensure that the council acts in an informed and lawful manner. Any queries regarding the use of NAFN should be referred to the Senior Responsible Officer's nominee set out in Appendix 2 who acts as the council's main point of contact with NAFN. The use of NAFN by local authorities is required by CoP s8.1- 8.2).

As the council's SPoC, NAFN will also:

- Provide quality assurance checks to ensure that applications consistently comply with IPA standards and to a sufficient level to meet OCDA and IPC scrutiny;
- Monitor those applications which are returned for rework or rejected by OCDA and determine the reasons why;
- Provide organisational and/or individual training as and where necessary sharing best practice advice and support;
- Be the point of contact between the council and the OCDA.

3 Verifying Senior Officers

The Code of Practice requires local authorities to ensure that someone of at least the rank of the Senior Responsible Officer in the local authority is aware of the application being made before it is submitted to an authorising officer in OCDA. The council's Senior Responsible Officer must be satisfied that the officer verifying the application is of an appropriate rank and must inform the NAFN of such nominations.

The council's designated verifying officers are listed in Appendix 2 and have been notified to NAFN. **Any application being submitted to NAFN must be verified by one of these officers.**

4 Office for Communications Data Authorisations (OCDA)

All local authority authorisations are made by the IPC (IPA sections 73 and 60A). Section 60A of the IPA conferred power on the IPC to authorise certain applications for CD. In practice the IPC has delegated these functions to its staff who sit in the OCDA. Applications made by the council are then submitted by NAFN on our behalf to the OCDA who will make decisions about those applications that strike a fine balance between the protection of privacy and risk to public safety. The OCDA will ensure that applications are assessed independently, rigorously and in line with the IPA. Applicants can not contact OCDA direct.

5 A Judicial Commissioner

A Judicial Commissioner is a person who holds or has held a judicial office, appointed under s227 IPA, who is responsible for approving requests to identify or confirm journalistic sources.

G Applications for Communications data

Communications data may only be acquired if the proper IPA approval process is followed. A more detailed flowchart is included in Appendix 1.

1 Making an Application (CoP 5.3-5.5)

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.

An application to acquire communications data must:

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

- specify the purpose for which the data is required, by reference to a statutory purpose under the IPA on the basis that they are satisfied that the request is undertaken in connection with a local authority function and that it is necessary for the applicable crime purpose depending on the category of data (including a consideration regarding the seriousness of the offence if applicable) (CoP 3.29-3.33);
- include a unique reference number;
- include the name and the office, rank or position held by the person making the application;
- describe whether the communications data relates to a victim, a witness, a complainant, a suspect, next of kin, vulnerable person or other person relevant to the investigation or operation;
- include the operation name (if applicable) to which the application relates;
- identify and explain the time scale within which the data is required;
- present the case for the authorisation in a fair and balanced way. In particular, all reasonable efforts should be made to take account of information which supports or weakens the case for the authorisation;
- consider 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;
- consider whether accessing the communications data is necessary;
- consider whether what is sought to be achieved could reasonably be achieved by other less intrusive means
- consider and, where appropriate, describe any meaningful collateral intrusion – the extent to which the rights of any individual not under investigation may be infringed and why that intrusion is justified in the circumstances (CoP 3.14-3.28);
- consider and, where appropriate, describe any possible unintended consequences of the application;
- consider whether the level of protection to be applied in relation to obtaining communications data is higher because of the particular sensitivity of that information;
- take account of the public interest in the integrity and security of telecommunications systems and postal services, and any other relevant aspect of the public interest in the protection of privacy;
- where data is being sought from a telecommunications operator or postal operator, specify whether the telecommunications operator or postal operator may inform the subject(s) of the fact that an application has been made for their data.
- include details of the officer verifying the application

The application will need to be verified by a council officer as identified in appendix 2. The officer carrying out the verifying function will also need to consider and be satisfied about the issues referred to in this paragraph when looking at the application.

2 Consultation with the SPoC - The National Anti Fraud Network (NAFN) (CoP 5.6-5.15)

Once verified, the Applicant will then send the Application Form to NAFN who will review it. 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 to the OCDA for authorisation.

3 Authorisation by the OCDA

The OCDA 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. They will make their decision based on the application that is made.

If the OCDA does not consider the criteria for obtaining data have been met the application will be rejected and referred back to the SPoC. The Applicant can then decide whether or not to proceed with the request, and if appropriate to resubmit a revised application or to resubmit the same application seeking a review of the decision by the OCDA.

If the application is approved, NAFN as the 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.

H Duration, renewals and cancellations (CoP Chapter 7)

1 Duration of authorisations

An authorisation becomes valid on the date upon which the authorisation is granted and is then valid of a maximum of one month.
This means that the conduct authorised should have been commenced within that month.

Where the authorisation or notice relates to the acquisition or obtaining of specific data that will be generated in the future, that future period is restricted to no more than one month from the date upon which the authorisation was granted or the notice given.

2 Renewal of authorisations (CoP 7.7 – 7.9)

Any valid authorisation may be renewed for a period of up to one month by the grant of a further authorisation. A renewed authorisation takes effect from the expiry date of the authorisation it is renewing.

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 or officer availability). Renewal may be appropriate where there is a continuing requirement to acquire or obtain data that will or may be generated in the future. The reasons for seeking the renewal should be set out by the Applicant in an addendum to the original application.

NAFN will liaise with the council 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.

The reasons, date and time of the renewal must be recorded.

3 Cancellation of authorisations (CoP 7.10-7.17)

Where an Applicant, verifying senior officer or NAFN become aware or consider that an authorisation is unnecessary or no longer proportionate, it should be withdrawn, NAFN should cease the authorised conduct and inform the OCDA.

A notice given under an authorisation is cancelled if the authorisation is cancelled but is not affected by the authorisation ceasing to have effect at the end of the one month period of validity. NAFN will notify the CSP of the cancellation.

I Data Protection Requirements (CoP Chapter 13), Records and Retention

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 2018 (DPA) and should be stored securely.

J Record Maintenance (CoP Chapter 24)

The council must keep a detailed record of all Applications, Authorisations, Withdrawals, Renewals and Cancellations . Records kept by the council must be held centrally by the SPoC. 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 as set out in the CoP Chapter 24. These records must be sent in written or electronic form to the IPC as requested by them.

3. Data Protection

Communications data, and all copies, extracts and summaries of it, must be handled and stored securely in accordance with the DPA 2018 and UK GDPR. Data must be effectively protected against unauthorised access and use, with particular consideration given to the principles of data security and integrity.

Departments that make applications for access to communications data should ensure that their records of the application and any subsequent 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 IPA and the DPA and the Communications Data Code of Practice. The Council must only disclose CD acquired under the IPA to the minimum extent necessary and when sharing data must be satisfied that the data will be adequately protected and that safeguards are in place to ensure this.

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.

Where it is necessary to process CD acquired under the IPA, the council must ensure that this is carried out in accordance with the data protection principles and must ensure that appropriate measures are in place to prevent unauthorised or unlawful processing and accidental loss or destruction of, or damage to, this data. Officers should have regard to the information available on the Source from the Information Governance team in relation to data protection principles, data management and security.

4. Document retention

CD may only be held for as long as it is still necessary for a statutory purpose and where it is no longer necessary or proportionate to hold such data, all copies of the relevant data must be destroyed.

5. Records

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.

The OCDA will only retain the CD applications and Decision Documents sent to them for a limited time. The council is therefore required to keep records of both the CD applications

that they issue as well as the decisions received from the OCDA. NAFN retain copies of applications and authorisations on behalf of the council.

6. Errors (CoP 14.4-14.6 & 24.17 – 24.37)

Where any error occurs in the granting of an authorisation, the giving of a notice or as a consequence of any authorised conduct, a record should be kept. NAFN keeps a record of any errors on the council's behalf.

Where an error results in CD being acquired or disclosed wrongly, this is a "reportable error" and a report and explanation is sent by NAFN's Senior Responsible Officer to the IPC as soon as is practical.

K Offences (CoP 15.6 – 15.18)

The IPA creates two offences which are relevant to the acquisition and disclosure of communications data:

- **Acquisition offence**: it is an offence for a person in the council to knowingly or recklessly obtain CD from a telecommunications operator or postal operator without lawful authority. This is not designed to capture errors on behalf of the council but rather instances where a person in the council failed to take account of obvious risk or where there is a deliberate failure to obtain an authorisation;
- **Disclosure offence**: it is an offence for a telecommunications operator to disclose without reasonable excuse the existence of an authorisation or notice for communications data by a public authority under the IPA.

L Oversight, Review and Amendments to the Policy and Procedures

1 External oversight

The Investigatory Powers Commissioner ensures compliance with the law by inspecting public authorities and investigating issues. Some serious errors must be reported to them and if they uncover serious errors they may inform the person affected. The IPC report annually. The Information Commissioner provides independent oversight of the integrity, security or destruction of data retained under Part 4 of the IPA and considers complaints about data protection. The Investigatory Powers Tribunal has jurisdiction to consider and determine complaints regarding public authority use of investigatory powers

2 Oversight Procedures

The Senior Responsible Officer (SRO) shall establish and maintain regular meetings not less than twice a year with the Verifying Senior Officers 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 Verifying Senior Officers. Such information and conclusions shall also be reported to the audit, governance and standards committee.

3 Review

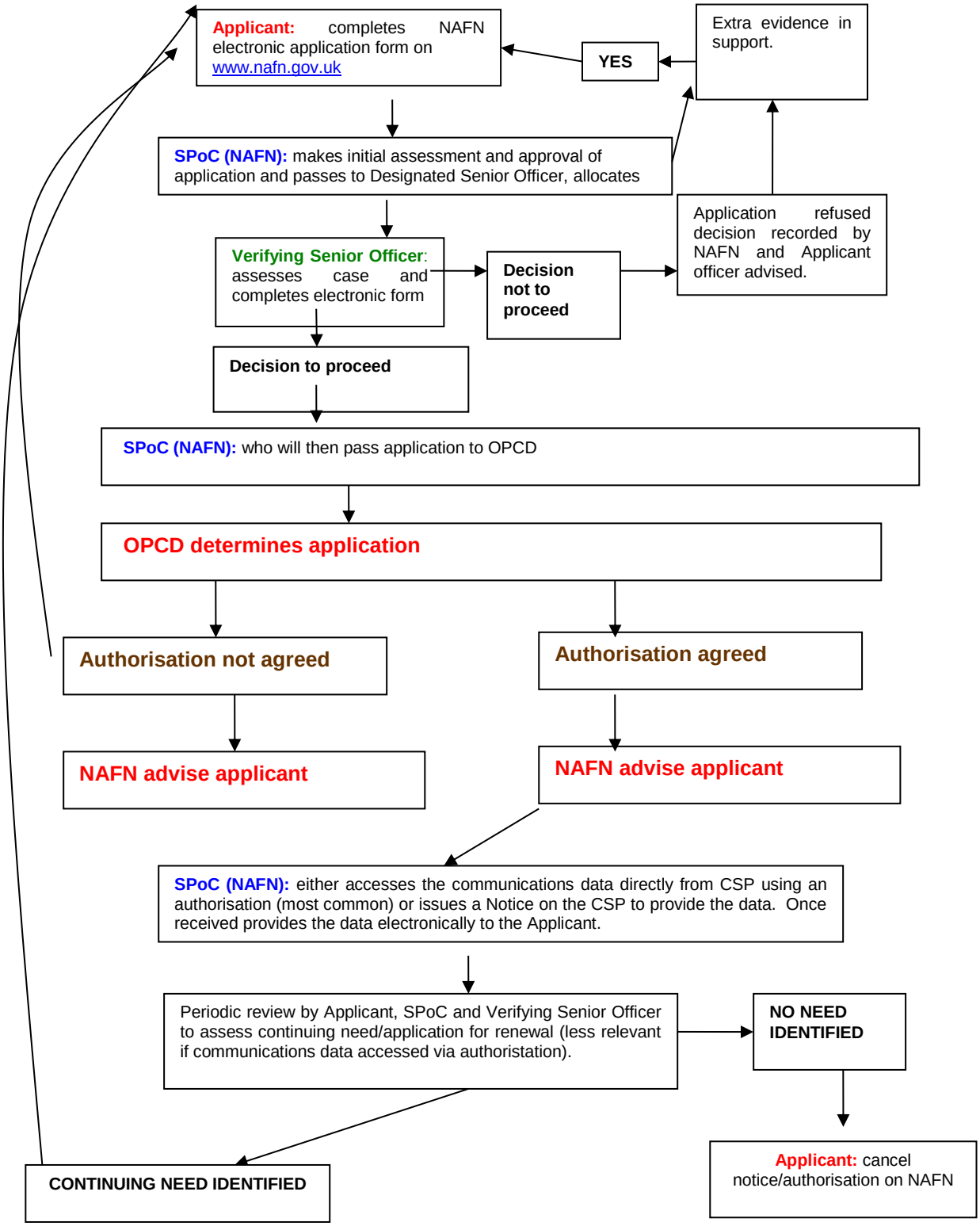
This policy will be reviewed every two years and approved by the relevant cabinet member. The members of the audit, governance and standards committee shall review the use of the Investigatory Powers Act 2016 and this policy at least once a year. In order to facilitate this,

the SRO shall provide regular reports to audit, governance and standards committee meetings on how the IPA has been used in the previous months and whether there are any concerns as to the policy.

4 Amendments to this Policy and Procedures

The SRO 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 Officers set out in Appendix 2, by adding, deleting or substituting any posts.

Appendix 1 Flow Chart of Communications Data Process



CD APPLICATION PROCESS

APPLICANT

1) Create a CD application as normal recording the statutory purpose of 60A(7)(b) for the applicable crime purpose.

EXAMPLE

This application is to support an investigation into fly-tipping under the Environmental Protection Act 1990. This meets the 12+ month's imprisonment definition of serious crime because the offence has a maximum sentence of five years.

2) On the application, record as part of the necessity case:
- a description of the offence(s) under investigation; and
- a justification for the seriousness of the offence (record which serious crime definition is met and how it is met, or record that the crime is not serious)

LOCAL AUTHORITY ONLY

APPROVED RANK OFFICER

DEFINITIONS OF SERIOUS CRIME

- 12 Month's+ Imprisonment: an offence that is capable of attracting a prison sentence of 12 months or more.
- Corporate Body: an offence by a person who is not an individual (i.e. a corporate body).
- Section 263 Offence: an offence falling within the definition of serious crime in section 263(1) of the Act (i.e. where the conduct involves the use of violence, results in substantial financial gain or is by a large number of persons in pursuit of a common purpose).
- Communication Offence: an offence which involves, as an integral part of it, the sending of a communication.
- Breach of Privacy: an offence which involves, as an integral part of it, a breach of a person's privacy.

3) Check that the public authority is permitted to use the recorded statutory purpose.

SPOC

4) Determine the conduct to satisfy the applicant's need (the type of data that is required)

5) If event data is required and the statutory purpose is crime, check the applicant has recorded:
- a description of the offence(s)
- a justification for the seriousness of the offence(s)

If not, return the application for rework.

6) Check the public authority is permitted to use the recorded statutory purpose

7) If the application is for event data and the statutory purpose is crime, check the seriousness of the crime has been justified. If not, reject or return the application for rework.

OCDA

Appendix 2 - Designated Officers referred to in the policy

Designation	Name	Title	Rank	Service Department
Senior Responsible Officer's Nominee	Allan Wells	Specialist Governance Lawyer	N/A	Law and Democracy
Verifying Senior Officer	Stephen Gaskell	Director of Strategy and Economy	Director	Chief Executive
Verifying Senior Officer	Dominic Cain	Director of Exchequer	Director	Exchequer Services
Verifying Senior Officer	Matt Clubb	Director of Environment	Director	Environment
Verifying Senior Officer	Toni Ainge	Director of Leisure	Director	Environment and Leisure

The officers listed above have been notified to NAFN and no other officers are authorised to act in these roles under any circumstances. Proposed changes or additions to the list of Verifying Senior Officers must be approved by the Senior Responsible Officer who will notify those amendments to NAFN.