April 2016

Policy and Procedures Document for the acquisition of Communications Data using The Regulation of Investigatory Powers Act 2000 (RIPA)

CHELTENHAM
BOROUGH COUNCIL

www.cheltenham.gov.uk

CONTENTS

1. BACKGROUND

1.1. The Council has a procedural guide for the use of RIPA which has been in place for some time and it should be noted that this document does not replace it. Any officer considering the use of RIPA as part of an investigation should follow the original guidance in the first instance.

1.2. Since September 2014, Local Authorities can only access communications data via the National Anti-Fraud Network (NAFN):

'NAFN is a not-for-profit, non-incorporated body formed by its members to provide services which support their work in the protection of the public purse. Established in 1997, NAFN was created as a centre of excellence to provide data and intelligence to its members. This includes assisting members in the provision of effective corporate and financial governance.

NAFN works with its members and other stakeholders to enhance and expand its range of services. It maintains all data in a secure and confidential environment conforming to Government legislation and national best practice'
NAFN constitution

1.3. Whilst it is not compulsory to join NAFN per se, a Local Authority must be a paid up member in order to make use of its single point of contact (SPoC) service in relation to communications data. The Council is a member, primarily to make use of other services provided by NAFN (credit referencing, DVLA checks, debtor tracing etc.) but given that Officers could now utilise the RIPA SPoC service and obtain communications data, guidance needs to be in place to govern the process.

1.4. This procedural guide is based on the requirements of The Regulation of Investigatory Powers Act 2000 (RIPA) and the Home Office Code of Practice on the Acquisition and Disclosure of Communication Data. The Council takes responsibility for ensuring its RIPA procedures are continuously improved and asks that any Officers with suggestions contact the RIPA Coordinator in the first instance. If any of the Home Office Codes of Practice change, the appropriate guide will be updated, and the amended version placed on the internet / published accordingly. Regular training sessions will also be provided to ensure that staff members are fully conversant with the Act.

1.5. Part 1 Chapter 2 of RIPA controls the obtaining of communications data by Local Authority staff. This data does not include the content of the communications i.e. the actual email message, letter, text or telephone conversation.

1.6. Part 1 also introduces a statutory framework to regulate access to communications data by Public Bodies consistent with the Human Rights Act 1998. It explains the duties and responsibilities placed upon each party involved in these processes. In addition it puts safeguards in place to balance the rights of the individual against the needs of society, as a whole, to be protected from crime and other public safety risks. This thus reflects the requirements of Article 8 of the European Convention on Human Rights; the right to privacy.

1.7. Communications data obtained under RIPA will be a justifiable interference with an individual's human rights, as above, provided such conduct is authorised, is both necessary and proportionate, and is in accordance with the law.

1.8. Therefore no Officer of the Council should require or invite a postal or communications operator to disclose data through the use of any other statutory duty or by exercising an exemption to the principle of non-disclosure under the Data Protection Act 1998. Another statutory power may only be used if it explicitly provides for the obtaining of telecommunications data.

1.9. In terms of internal monitoring of communications data, emails, internet usage etc. it is important to recognise the interplay and overlap with the Council's ICT Policies and the Data Protection Act 1998 (to include the Codes of Practice). Under normal circumstances the Council's Policies should be adhered to as any such monitoring is permitted as per Contracts of Employment and Codes of Conduct. All electronic data held internally is deemed to be of a business nature and may therefore be accessed without further notice; RIPA authorisation is not therefore required. However, advice should be obtained if there are any significant implications which could impact a person's private life. In those circumstances it may be prudent to complete a Non-RIPA Authorisation Form to consider any human rights issues which must be retained on the central register.

2. DEFINITION OF COMMUNICATIONS DATA AND CATEGORISATION

2.1. Communication data means any traffic or any information that is or has been sent over a communications system or postal system, together with information about the use of the system made by any person. In effect the term communications data embraces the "who, when and where" of a communication but not the content, not what was said or written. It can include the address on an envelope, the time and duration of a communication, the telephone number or e- mail address of the originator and recipient, unanswered call attempts and the location from which the communication was made. It includes the manner in which and by what method a person (or machine) communicates with another person (or machine), but excludes what they say or data they pass on, including text, audio and video. The content of such communications is covered by Interception of Communications Legislation.

2.2. An operator who provides a postal or telecommunications service is described as a Communications Service Provider (CSP).

2.3. Section 4 of the Data Retention and Investigatory Powers Act 2014 (DRIPA) clarifies that data access powers under RIPA are exercisable in respect of CSPs that are based outside of the United Kingdom, but provide services to the UK. Data retained under a Data Retention Notice under Section 1 of DRIPA can only be acquired in accordance with RIPA (or a Court Order).

2.4. RIPA defines communications data in three broad categories:

- Section 21(4)(c) Information about Communications Service Users:

This category is information held or obtained by a CSP about persons to whom communications services are provided. It mainly includes personal records supplied to the Communication Services Provider (CSP) by the customer/ subscriber. For example, their name and address, payment method, contact number etc.

- Section 21(4)(b) Information about the use of Communications Services:

This category is the data relating to the use made by a person of a communications service. It mainly includes everyday data collected by the CSP related to the customer's use of their communications system and which would be routinely available to the customer. For example, details of the dates and times they have made calls and which telephone numbers they have called.

- Section 21(4)(a) Information about Communications Data (Traffic Data):

This category is data that is or has been comprised in or attached to a communication for the purpose of its transmission. It mainly includes data generated by the Communications Service Provider (network data) relating to a customer's use of their communications system (that the customer may not be aware of), for example, cell site data and routing information.

3. COMMUNICATIONS DATA AVAILABLE TO LOCAL AUTHORITIES

3.1. The types of information that we are allowed to access from a CSP fall into two categories:

- Subscriber Information (RIPA S21(4)(c)) - Information about Communications Services Users:

Name of the customer who is the subscriber for a telephone number, an email account, PO Box number, a Post Paid mailing stamp, or is entitled to post to a web space;

Account information such as address for billing, delivery or installation;

Subscriber account information such as bill paying arrangements, including details of payments and bank or credit/ debit card details;

Information about the provision of forwarding and redirection services;

Information about connection, disconnection and reconnection of services the customer subscribes to, including conference calling, call messaging, call waiting and call barring telecommunications services;

Information provided by the subscriber to the CSP such as demographic information or sign up data (other than passwords) such as contact telephone numbers;

Information about telephones or other devices provided by the CSP to the subscriber and associated codes, including manufacturer and model, Personal Unlocking Keys for mobile phones & serial numbers;

Information that the CSP chooses to collect about the device being used by the customer;

Top-up details for pre-pay mobile phones including credit/ debit card, voucher/ e-top up details.

- Service Use Data (RIPA S 22(4)(b) - Information about the use of Communications Services:

Periods during which the customer used the service;

Activity including itemised records of telephone numbers called, Internet connections, dates and times of calls, duration of calls, text messages sent and quantities of data uploaded or downloaded;

Information about use made of forwarding and redirection services;

Information about the use made of conference calling, call messaging, call waiting and call barring telecommunications services;

Information about the selection of preferential numbers or discount calls;

Records of postal items; such as records of registered, recorded or special delivery postal items and records of parcel consignment, delivery and collection.

3.2. The Council is not allowed to access:

- Traffic Data (RIPA S 22(4}(a) - Information about the communications themselves:

Information identifying the sender and recipient of a communication (from data within the communication);

Information tracing the origin or destination of a communication including incoming call records;

Information identifying any location of any equipment making a communication, such as mobile phone cell site location;

Web browsing information such as the web sites visited (rather than the specific pages within that website) or servers used;

Routing information identifying equipment through which a communication has been transmitted (e.g. dynamic IP addresses, file transfer logs and email headers);

Addresses or markings, including sender or recipient, written on the outside of a postal item in transmission (such as a letter or parcel), that shows the items postal routing;

Online tracking of Communications, such as postal items.

3.3. Local Authority staff are only allowed to acquire and disclose communications data for the purpose of preventing or detecting crime or for preventing disorder. This

purpose should only be used in relation to the specific (and often specialist) offences or conduct that the Council has been given the statutory function to investigate. For communications data, the offence does not have to carry a six month tariff as with directed surveillance.

3.4. Where a joint investigation is being conducted between the Council and another enforcement authority, such as the police, either authority may, where necessary and proportionate, acquire any communications data under RIPA to further the joint investigation.

3.5. The purpose of this policy is to provide guidance for obtaining communications data now that the Council is a member of NAFN. The knowledge and experience of the NAFN Single Points of Contact (SPoC's) is essential and these SPoC's should be used to obtain advice and assistance as and when required. Such a discussion is particularly helpful when the Applicant is unsure of the category of data that they are seeking or the Applicant wants to find out more about what additional information may be retained by the CSP. However, final approval of the request is made by an authorising member of staff; the Designated Person(s) within the Local Authority.

4. POWER TO OBTAIN COMMUNICATIONS DATA

4.1. There are two powers granted by S22 RIPA in respect of the acquisition of communications data from telecommunications and postal companies or 'Communications Service Providers' (CSP's).

4.2. A notice under S22(4). In order to compel a CSP to obtain and disclose, or just disclose, communications data in their possession, a notice under S22(4) RIPA must be issued. The sole grounds to permit the issuing of a S22 notice by a Local Authority is for the purposes of 'preventing or detecting crime or of preventing disorder'. The issuing of such a notice is likely to be the main power utilised by a Local Authority, in those circumstances where the Council SPoC, being NAFN, liaises directly with the CSP.

4.3. An authorisation under S22(3). This power is to be used when a CSP cannot provide the information; there may be several reasons for this. An authorisation provides for persons within a public authority to engage in specific conduct, relating to a postal service or telecommunications system, to obtain communications data. Any designated person in a public authority may only authorise persons working in the same public authority to engage in specific conduct, such as requesting the data via secure auditable communications data acquisition systems. This will normally be the public authority's SPoC, though Local Authorities must now use NAFN.

4.4. Under S23A and S23B RIPA, judicial approval must also be granted for all Local Authority requests for communications data. This is outlined in more detail within this policy.

5. PROCEDURE FOR OBTAINING COMMUNICATIONS DATA

5.1. There is now only one method that officers can use to obtain communications data; by way of the NAFN secure website. To use this system Applicants have to

individually register on the NAFN website - www.nafn.gov.uk. A Designated Person will also need to be registered to authorise the Applicants requests. A number of departments within the Council have contributed towards the NAFN annual membership fee, any Applicant therefore needs to confirm with their Line Manager that they are allowed to register. Should you have any queries, please contact the Internal Audit Department.

5.2. Please note, if your department is part of a shared service, the Local Authority on whose behalf the request is being made must be a member of NAFN and the request made via login details for that Council. Applicants and Designated Persons cannot make use of one Local Authority's membership to obtain any information on behalf of another. Login details will be necessary for each Local Authority that an individual is employed by or works on behalf of.

5.3. Once an Applicant is registered with NAFN, as with other RIPA requests, the Applicant must complete an application for the communications data. This request is completed online and is submitted electronically to the SPoC's at NAFN. On this form the Applicant must provide the following information:

- Name and designation of Applicant;
- Include a unique reference number and, where applicable, the operation name;
- The purpose for which the data is required, which can only be for the prevention and detection of crime or preventing disorder;
- Details of the communications data required;
- Describe whether the communications data relates to a victim, a witness, a complainant, a suspect, a vulnerable person or other person relevant to the investigation;
- Time period for which the data is required, including historic or future data;
- Why it is necessary to obtain the data, including the source of the communications data address and what is expected to be achieved from obtaining the data;
- Why it is proportionate for the data to be obtained, including why the intrusion benefits the investigation and whether the level of intrusion can be justified against the individual's right to privacy;
- Details of whether there is any meaningful collateral intrusion and why that intrusion is justified;
- Consider and describe any possible unintended consequences of the application;
- Time scale within which the data is required (this can only be the routine non-urgent timescale i.e. Grade 3, unless there is a high level of urgency for obtaining the data, such as when life is in danger);
- The Applicant also confirms that they undertake to inform the SPoC of any changes in circumstances that no longer justify the acquisition of the data.

5.4. As with all RIPA applications, a request for communications data should only be made after all other avenues have been considered. It is therefore appropriate that the Applicant should indicate any open source checks that they have made on the

telephone numbers/ communications addresses already made to justify the principle of proportionality.

5.5. The Applicant is entitled to ask for historical data or may request future data, by which the CSP must provide details of, for example, all outgoing telephones or internet connections over a set future period of up to a month. Requests for such future data are considered to be more intrusive than requests for historical data.

5.6. It can be appropriate to obtain service use data at the same time as obtaining subscriber information, for example when the person who is the subject of the investigation is identified from high-grade intelligence to be using a specific number or service or when a mobile phone is lawfully seized. An application for subscriber information can be included in an application for service use data.

5.7. Once fully complete, the form can then passed electronically to the appropriate NAFN accredited Single Point of Contact for Accessing Communications Data (SPoC). The accredited SPoC's at NAFN provide independent scrutiny of the applications so it is important that the Applicant consults with a NAFN SPoC throughout the authorisation process. The NAFN SPoC will advise the Applicant of any amendments necessary.

5.8. After the NAFN SPoC considers the application to be satisfactory, the appropriate Designated Person will then receive an email to say that there is an application form on the website for him or her to consider. The Designated Person completes the relevant part of the form to provide approval.

5.9. At this time, the RIPA Coordinator / Senior Responsible Officer should be made aware that a request has been made so that the central register can be updated.

5.10. The NAFN SPoC then uses the authorisation process to obtain the required communications data from the CSP database. The data is posted on the NAFN website and can only be accessed by the Applicant. If NAFN do not have direct access to the database of the relevant CSP, the NAFN SPoC will send a notice to the CSP in the usual way.

5.11. The majority of information related to public sector business, operations and services can be managed as OFFICIAL; in the case of communications data this should be managed as OFFICIAL – SENSITIVE which identifies it as being subject to a 'need to know' basis thus limiting access to it. This does not preclude the lawful disclosure of material when required but does make clear that the information obtained must be treated with care, and also stored and handled in accordance with the Council's duties under the Data Protection Act.

5.12. Using NAFN to obtain communications data has significant advantages in comparison to the previous method in that the time in which the data can be obtained is significantly reduced, costs are kept to a minimum because the charges made by the CSP's for providing the data are considerably less when using NAFN and it ensures consistency across Local Authorities.

6. COMMUNICATIONS DATA RELATING TO CERTAIN PROFESSIONALS

6.1. Communications data is not subject to any form of professional privilege, since the fact that a communication has taken place does not disclose its contents. Clearly though the degree of interference with privacy may be higher where the communications data being sought relates to a person who is a member of a profession that handles privileged or otherwise confidential information (for example a medical doctor or lawyer). It may also be possible to infer an issue of sensitivity from the fact that someone has regular contact with someone like a lawyer or journalist.

6.2. Such situations do not preclude an application being made. Special consideration should be given to the issues of necessity and proportionality, drawing attention to any such circumstances that might lead to an unusual degree of intrusion or infringement of rights and freedoms, particularly privacy, and where it might be engaged, freedom of expression.

6.3. Applicants must clearly note in all cases when an application is made for the communications data of those known to be in such professions, including medical doctors, lawyers, journalists, Members of Parliament, or ministers of religion. That such an application has been made must be recorded, to include the profession, and, at the next inspection, such applications should be flagged to the Interception of Communications Commissioner's Office (IOCCO).

6.4. Issues surrounding the infringement of the right to freedom of expression may arise when a request is made for the communications data of a journalist. There is a strong public interest in the willingness of sources to provide information to journalists anonymously. If an application is intended to determine the source of journalistic information, there must be an overriding requirement for it to be in the public interest. Even if it is not intended to determine the source of journalistic information there is still a risk of collateral intrusion into legitimate journalistic sources, so particular care should be taken to properly consider the public interest in whether the intrusion is justified. This should include drawing attention to whether alternative evidence exists or whether there are alternative means to obtain the information. Identification of journalist sources can only be sought by using production orders under the Police and Criminal Evidence Act 1984 (PACE), which are not available to the Council. Judicial oversight does not apply where applications are made for the communications data of those known to be journalists, but where the application is not to determine the source of journalistic information, for example where the journalist is a victim of crime or is suspected of committing a crime unrelated to their occupation.

6.5. Communications data that may be considered to determine journalistic sources includes data relating to:

- Journalists' communications addresses;
- Communications addresses of those persons suspected to be a source;
- Communications addresses of persons suspected to be acting as intermediaries between the journalist and the suspected source.

7. PREPAID MOBILE PHONES

7.1. Unregistered prepaid mobile phones are common amongst criminals as it allows them to avoid detection more easily and it is thus possible that a subscriber check will identify a number as belonging to one of these devices. This does not necessarily prevent an investigating officer obtaining useful information.

7.2. The Applicant can ask for further information about the subscriber under section 21(4)(c) including top-up details, method of payment, bank account used or customer notes.

7.3. The Applicant should outline in their original application the further information that will be required if the phone turns out to be prepaid, so as to allow the widening of the data capture. This information could be requested in two stages: firstly asking for the subscriber details and then, if this turns out to be an unregistered prepaid phone, asking for the further information.

7.4. If the Designated Person approves the application it is recommended by IOCCO that he or she should approve the use of authorisations rather than the use of notices, whereby the authorisation should state that the SPoC is authorised to engage in any conduct to acquire information about the user that is covered by Section 21(4)(c). Under the legislation an authorisation does not have to be issued by the Designated Person so it can be issued by the SPoC.

7.5. The SPoC will then serve an appropriate authorisation on the relevant CSP. If further information is required the SPoC will need to serve another authorisation on the CSP requesting the additional information. It should be noted that each authorisation will bear the date that the Designated Person approved the original application. This streamlining process is more efficient than using notices, because otherwise a request for each additional notice would need to be referred to the Designated Person.

7.6. The information that is received can then be developed to try to obtain further information about the user of the phone. Solution Providers such as EasyPay, EPay etc. are the third parties involved in the transaction of credit placed on a mobile phone. If a Solution Provider is provided with the mobile telephone number, the transaction date and the transaction number, they are often able to provide the method of payment and the location of the top-up. Solution Providers are not CSPs and therefore they cannot be issued with a notice under RIPA; instead the data can be applied for under the Data Protection Act.

8. HOME OFFICE GUIDANCE

8.1. The Home Office has provided guidance in relation to the acquisition of communications data namely ‘Guidance for the layout of a Chapter II Application Form and; Guidance for Applicants and Designated Persons considering necessity and proportionality’.

8.2. The guidance was produced jointly by the Home Office and the Data Communications Group (DCG) in conjunction with the IOCCO. The full document is available online should it be required.

8.3. The Home Office also produced a Code of Practice and various revisions have taken place. Relevant extracts are detailed below taking in to account the guidance and Code of Practice. The Council and those persons acting under RIPA must have regard to the Code of Practice on the Acquisition and Disclosure of Communications Data issued by the Home Office under the Act. The full document is available online.

8.4. **COMMUNICATIONS DATA:** An application, comments by the Single Point of Contact (SPoC), considerations of the Designated Person, authorisations and notices may be made in writing ('paper') or electronically ('database').

8.5. It may be appropriate for the section 'communications data' within the application form to include 'text boxes' to enable the applicant to set out the:

- Telephone number, email address, etc;
- Where appropriate the 'between times/ dates' of the data set required;
- Type of data required, for example subscription details, outgoing calls, incoming calls.

8.6. An application may contain several requests for various 'data sets' relating to a specific investigation or operation. However, consideration should be given as to how this may affect the efficiency of the public authority's processes and the impact of managing disclosure issues before, during and after a criminal trial.

8.7. **NECESSITY:** In order to justify the application is necessary the applicant needs as a minimum to consider three main points:

- The *event* under investigation, such as a crime or vulnerable missing person;
- The p*erson*, such as a suspect, witness or missing person and how they are linked to the event;
- The *communication data*, such as a telephone number or IP address, and how this data is related to the person and the event.

8.8. In essence, necessity should be a short explanation of a) the event, b) the person and c) the communications data and how these three link together. The application must establish a link between the three aspects to be able to demonstrate the acquisition of communications data is necessary for the statutory purpose specified.

8.9. Necessity does not entail explaining 'what will be achieved by acquiring the data' or 'why specific time periods have been requested' - these points are relevant to proportionality and should be covered in the relevant section to stop repetition.

8.10. **PROPORTIONALITY:** Applicants should include an outline of how obtaining the data will benefit the investigation or operation. If more than one item of data is being sought, the relevance of the additional data should be explained.

8.11. This outline should include explaining how the level of intrusion is justified when taking into consideration the benefit the data will give to the investigation. This justification should include confirmation that relevant less intrusive investigations have already been undertaken where possible. For example the subscriber details of

a phone number may be obtained from a phone book or other publically available source.

8.12. The relevance of any time periods requested must be explained, outlining how these periods are proportionate to the event under investigation. The two basic questions are:

- What are you looking for in the data to be acquired and;
- If the data contains what you are looking for, what will be your next course of action.

8.13. An explanation as to how communications data will be used, once acquired, and how it will benefit the investigation or operation, will enable the Applicant to set out the basis of proportionality.

8.14. An explanation of the proportionality of the application should include a consideration of the rights (particularly to privacy and, in relevant cases, freedom of expression) of the individual and a balancing of these rights against the benefit to the investigation.

8.15. An examination of the proportionality of the application should also involve consideration of possible unintended consequences and, when relevant this should be noted. Unintended consequences of an application are outcomes that are not intended by the application. Unintended consequences are more likely in applications for the data of those professions with duties of confidentiality. For example, if a journalist is a victim of crime, applications for service use data related to that journalist's phone number as part of the criminal investigation may also return some phone numbers of that journalist's sources, with unintended impact on freedom of expression. Such an application may still be necessary and proportionate but the risk of unintended consequences should be considered.

8.16. **COLLATERAL INTRUSION:** Consideration of collateral intrusion forms part of the proportionality considerations and becomes increasingly relevant when applying for traffic data or service use data. Applications should include details of what collateral intrusion may occur and how the time periods requested impact on the collateral intrusion. When there are no meaningful collateral intrusion risks, such as when applying for subscriber details of the person under investigation, the absence of collateral intrusion should be noted.

8.17. The question to be asked is ‘Will the data set to be acquired result in collateral intrusion to persons outside the line of enquiry the data is being obtained for?’ For example itemised billing on the subject's family home will be likely to contain calls made by the family members.

8.18. Applicants should not write about a potential or hypothetical ‘error’ and if the Applicant cannot identify any meaningful collateral intrusion, that factor should be recorded in the application i.e. ‘none identified’.

8.19. **TIME SCALE:** Completion of this section within the application form assists the SPoC to prioritise the request.

8.20. DCG has an agreed Grading System that indicates to the CSP any urgent timescales, which is synchronised with the Urgent Oral Process (see Home Office Acquisition and Disclosure of Communications Data Code of Practice).

8.21. **ROLE OF THE SPOC:** The Home Office must accredit all SPoCs, and this involves attendance on a recognised training course, the passing of an examination and being issued with a SPoC Personal Identification Number. The SPoC ensures that only practical and lawful requests for communications data are undertaken.

8.22. All notices and authorisations for communications data must be channelled through SPoC at NAFN. This is in order to provide an efficient regime since the SPoC will deal with the CSP's on a regular basis.

8.23. The SPoC (in this case NAFN) will receive the application form and will advise Applicants and Designated Persons on the following:

- Whether the forms have been filled in correctly and are lawful;
- Whether the data requested falls within Section 21(4) (a), (b) or (c) of the act;
- Whether access to the communications data is reasonably practical for the CSP or whether the specific data required is inextricably linked to other data;
- Whether there are likely to be any possible unintended consequences of the application;
- The practicalities of accessing different types of communications data from different telecommunications or postal operators;
- Whether data disclosed by a CSP fulfils the requirements of the notice;

8.24. The SPoC will assess the Application for Communications Data form and on it record the following:

- If the request is not reasonably practical for the SPoC the reason why this is so;
- Whether the data falls into Section 21(4) (a), (b) or (c) of the act;
- Whether a notice or authorisation is appropriate;
- Any adverse cost implications to the CSP or the Local Authority;
- Details of any data that is likely to be obtained in excess of the data requested;
- Any other factors that the Designated Person should be aware of;
- Description of the data to be acquired and, where relevant, specifying whether any historic or future data is required and the time periods sought;
- Identifying the relevant CSP.

8.25. The SPoC will issue a Unique Reference Number for the form. The SPoC will draft the relevant notice or authorisation to be submitted for approval to the Designated Person. The SPOC will keep a chronological record of the processing of the application including any contacts made by him or her with the CSP's. He or she may also give a priority grading to the CSP depending on the urgency of the application.

8.26. NAFN employ a number of officers as SPoCs and they can be contacted directly at the NAFN Offices to discuss any issues.

8.27. If the Council needs to request information from a CSP that does not consist of communications data, it is good practice to use the NAFN SPoC to liaise with the CSP on such requests.

8.28. **CONSIDERATIONS OF THE SPOC:** If the application is being recorded within a database (or other electronic format), and is attributable to the applicant, a signature is not required.

8.29. An application, comments by the single point of contact (SPOC), considerations of the Designated Person, authorisations and notices may be made in writing ('paper') or electronically ('database').

8.30. The question 'Describe the communications data to be acquired specifying, where relevant, any historic or future date and/or time periods sought', is appropriate where the communications data sought by the Applicant may need refinement by the SPOC. For example incoming calls to a telephone number held by a CSP that does not keep a data set that can reveal such calls. The SPOC would state that several authorisations and notices will need to be undertaken with CSPs that can reveal calls instigating from the networks to the telephone number in question.

8.31. The Designated Person, having considered the comments of the SPoC, may decide the acquisition is not justified because of the significant resources required by the CSP to retrieve and disclose the data or it will be impractical for the public authority to undertake an analysis of the data.

8.32. It will also be appropriate for the SPoC to comment where the data sought by the Applicant will require the acquisition of excess data, specifically where it is not practicable for the CSP to edit or filter the data, for example a specific incoming call in a data set with outgoing calls and cell site contained in it. If the Designated Person considers this to be necessary and proportionate for the acquisition of the specific incoming call then the authorisation or notice must specifically include the acquisition of the outgoing call, incoming calls and cell site.

8.33. **APPROVAL BY THE DESIGNATED PERSON:** The SPoC will submit the Application for Communications Data Form, along with the relevant draft notice(s) or authorisation(s), to a Designated Person, who will make the decision about whether or not the application will be approved.

8.34. The Designated Person must be one of those officers, of a suitable rank, who are currently Authorised Officers under RIPA, so they are already able to approve surveillance or CHIS applications. In no cases may someone be both the Designated Person and the Applicant.

8.35. Designated Persons must have current working knowledge of human rights principles, specifically those of necessity and proportionality, and how they apply to the acquisition of communications data.

8.36. Designated Persons must be independent from the operation or investigation when granting authorisations or giving notices relating to those operations. The Designated

Person must not be directly responsible for the operation or investigation i.e. they should not have a strategic or tactical influence on the investigation. In effect the Designated Person should be far enough removed from the Applicant's line management chain, which will normally mean they are not within the same department or unit. The name of the Designated Person will be given to NAFN and any application requiring approval will be sent direct.

8.37. In circumstances where the Council is not able to call on the services of an independent Designated Person, the Senior Responsible Officer must inform IOCCO of the circumstances and reasons. This could include a small specialist investigation service within the Council, for example applications which relate to corporate fraud and/or internal investigations. The justification for using a non-independent Designated Person and their involvement in the investigation must be explicit in their recorded considerations. Any use of non-independent Designated Persons must be notified to IOCCO during any inspections. The submission to IOCCO of the notification of exemption form is considered to be sufficient for these purposes.

8.38. The Designated Person will consider the form and then complete the Designated Person's part of the Application Form to state whether they grant or refuse the application. On the form the Designated Person must record the following:

- Why he/she believes acquiring the communications data is necessary;
- Why he/she believes the conduct involved in acquiring the communications data is proportionate;
- If accessing the communications data involves a meaningful degree of collateral intrusion, why he/she believes that the request is still proportionate.

8.39. When considering proportionality the Designated Person should apply particular consideration to unintended consequences.

8.40. The decision of the Designated Person must be based on the information presented to them in the application. If the application is approved, the Designated Person can authorise the accessing of communications data by one of two methods as follows:

- By a notice under RIPA S 22(4), which is a notice given to the postal or telecommunications operator and requires that operator to collect or retrieve the data and provide it to the Authority that served the notice.
- By an authorisation under RIPA S 22(3), which allows the Authority to collect and retrieve the data itself. It is extremely unlikely that we will make use of this, as this is only intended to be used if the operator is incapable of complying with a notice, or if the Authority will retrieve the data using an on-line system.

8.41. The Designated Person should specify the shortest time period for the data that is necessary in order to achieve the objective for which the data is sought.

8.42. The Designated Person shall endorse the draft notice or authorisation with the date, and if appropriate the time, at which he or she gives the notice or authorisation. This is the point at which the Designated Person approves the application.

8.43. If the Designated Person wishes for any advice they are able to obtain it from the NAFN SPoC.

8.44. At the time of giving a notice or granting an authorisation to obtain specific service use information, the Designated Person may also authorise the consequential acquisition of specific subscriber information relating to the service use data that is to be obtained. This must only be to the extent that is necessary and proportionate at that time, such as to identify with who a person has been in communication.

8.45. If the application is rejected either by the SPoC or the Designated Person, the SPoC will retain the form and inform the Applicant in writing and include the reasons for its rejection. The RIPA coordinator will also need to be informed of any rejected applications so that the central register can be updated.

8.46. Once the application has been authorised by the Designated Person the authorisation then needs to receive judicial approval from a magistrate. Further information is set out at within the section detailed 'Judicial Approval'.

8.47. **CONSIDERATIONS OF THE DESIGNATED PERSON:** The Designated Person must be able to show he or she has understood the need for the application and considered necessity and proportionality to a standard that will withstand scrutiny.

8.48. The Designated Person should tailor their comments to a specific application as this best demonstrates the application has been properly considered.

8.49. If the Designated Person having read the application considers the Applicant has met all requirements, then he or she should simply record that fact. In such cases a simple note by the Designated Person should be recorded.

8.50. There may be circumstances where the Designated Person having read the case set out by the Applicant and the considerations of the SPoC will want to comment why it is still necessary and proportionate to obtain the data despite excessive data being acquired.

8.51. If the Designated Person does not consider the case for obtaining the data has been met the application should be rejected and referred back to the SPoC and the Applicant.

8.52. A notice must include a unique reference number that also identifies the public authority. This can be a code or abbreviation.

8.53. If the Designated Person is recording their considerations within a database (or other electronic format) and is attributable to the Designated Person, a signature is not required.

8.54. **NOTICES AND AUTHORISATIONS:** The NAFN SPoC will supply the Designated Person with a draft notice or authorisation. Where a notice needs to be issued, the NAFN SPoC will produce the notice on behalf of the Designated Person. All notices and authorisations should refer to data relating to a specific date or period of time. If the date is specified as 'current', the data should be provided by the CSP as at the

date of the notice. The notice should give enough information to the CSP to allow them to comply. There is no need to produce a separate notice for each communications address, when these addresses all relate to the same CSP.

8.55. The notice is then served on the CSP by the relevant SPoC. The SPoC will give the notice a Unique Reference Number that cross-references it to the application that was granted.

8.56. The SPoC is responsible for all contacts between the Authority and the CSP.

8.57. Authorisations will mainly be utilised when carrying out the streamlining process for prepaid phones. The SPoC will generate the authorisation on behalf of the Designated Person. The NAFN SPoC will be able to obtain the communications data from the CSP database. Legally the authorisation does not need to be served on the CSP. However the CSP may require or be given an assurance that the conduct undertaken is lawful. That assurance may be given by disclosing details of the authorisation or by providing the actual authorisation.

8.58. Once the data is obtained, the SPoC will provide the data to the Applicant, but the SPoC can filter out any unnecessary information provided by the CSP. The SPoC will retain the original data obtained from the CSP (known as the 'golden copy') and provide a copy of it to the Applicant. This golden copy is capable of being provided to the CSP in the future, in order to enable a witness statement to be obtained in circumstances where the CSP no longer retains their original data. The Applicant should keep the data that they receive in a secure manner, in order to comply with Data Protection requirements.

8.59. The CSP must comply with the requirements of a notice, as long as it is reasonably practical for them to do so. Under S24 of RIPA, the CSP is entitled to recover the reasonable costs of making 'timely disclosure' of such data. Ordinarily the CSP should disclose the required communications data within ten working days of the notice being served on them, but if in specific circumstances where this would not be possible the Designated Person may specify a longer period of up to a month.

8.60. All notices and authorisations will only be valid for a month, but they may be renewed by the Designated Person for further periods of a month, at any time within the current life of the notice or authorisation. This should be set out by the Applicant in an addendum to the original application.

8.61. If the need for the communications data ends, or obtaining the data is no longer proportionate, the Designated Person must cancel the notice using a cancellation form, before data is provided by the CSP. This cancellation notice is sent to the CSP.

8.62. In a similar manner an authorisation must be withdrawn and, if appropriate, the CSP should be advised of this withdrawal. In the NAFN system this is done via the website. However the notices (and authorisations) terminate when the CSP provides the requested data, so there is usually no need for a cancellation form to be completed.

8.63. All original documents will be retained as required by the business need and in accordance with the Council's data retention policies.

8.64. **JUDICIAL APPROVAL:** Once an application for the acquisition and use of communications data has been authorised by the Designated Person, the authorisation or notice then needs to receive judicial approval from a Magistrate. The Applicant will need to download the authorised version of the application form from the NAFN website along with the judicial approval forms and take these forms to the Magistrates' Court.

8.65. The Applicant will need to contact the Magistrates' Court to arrange an appointment for the application to be made. The Applicant will complete the judicial approval application form (Form JA1) and prepare a judicial approval order form (Form JA2) for signature by the Justice of the Peace (JP). The application form will contain a brief summary of the circumstances of the case.

8.66. The officer will provide the JP with a copy of the original RIPA authorisation or notice and the supporting documents setting out the case. This forms the basis of the application to the JP and should contain all information that is relied upon. The original RIPA authorisation should be shown to the JP but it will be retained by the Local Authority. The Court may wish to take a copy. The partially completed judicial application and order forms will be provided to the JP.

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

8.68. The JP will consider whether he or she is satisfied that at the time the authorisation or notice was granted or renewed there were reasonable grounds for believing that the authorisation or notice was necessary and proportionate. They will also consider whether there continues to be reasonable grounds.

8.69. The forms and supporting papers must by themselves make the case. It is not sufficient for the officer to provide oral evidence where this is not reflected or supported in the papers provided. The JP may note on the form any additional information he or she has received during the hearing but the request should not be submitted in this manner.

8.70. If more information is required to determine whether the authorisation or notice has met the tests then the JP will refuse the authorisation or notice. If an application is refused the Local Authority should consider whether they can reapply using additional information available that had not initially been included within the papers provided at the hearing.

8.71. The JP will record his or her decision on the judicial order form. This will be the official record of the JP's decision. Court staff will securely retain a copy of the RIPA authorisation and the judicial application and order forms.

8.72. The decisions that the JP can make are as follows:

- Approve the grant or renewal of the authorisation or notice;
- Refuse to approve the grant or renewal of an authorisation or notice;
- Refuse to approve the grant or renewal and quash the authorisation or notice.

8.73. If the JP refuses to grant or renew the authorisation or notice it will not take effect and the Local Authority may not use the technique in that case.

8.74. Where an application has been refused the Council may wish to consider the reasons for that refusal. For example, a technical error in the form may be remedied without the Council going through the internal authorisation process again. The officer may then wish to reapply for judicial approval once those steps have been taken. If the JP 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 two business days from the date of the refusal in which to make representations.

8.75. The Council will need to obtain judicial approval for all initial RIPA authorisations or notices. In addition to the application form etc. officers will need to retain a copy of the judicial application and order forms after they have been signed by the JP. There is no requirement for the JP to consider either cancellations or internal reviews.

8.76. On rare occasions officers might have the need for out of hour's access to a JP so the officer will need to make the necessary arrangements with the Court staff. The officer will need to provide two partially completed judicial application and order forms so that one can be retained by the JP. The officer should provide the Court with a copy of the signed judicial application and order forms the next working day.

8.77. Where renewals are timetabled to fall outside of Court hours, for example during a holiday period, it is the investigating officer'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.

8.78. Should judicial approval be granted, the officer will need to provide the judicial approval form to the NAFN SPoC.

8.79. **ERRORS:** Where any error occurs, in the giving of a notice or authorisation or as a consequence of any authorised conduct or any conduct undertaken to comply with a notice, a record should be kept. An error can only occur after the notice has been served on the CSP, so if it is discovered before this point it does not officially count as an error. There are two types of errors namely reportable errors and recordable errors:

- Reportable errors are ones where communications data is acquired wrongly and in this case a report must be made to the IOCCO, as this type of occurrence could have significant consequences for the individual whose details were wrongly disclosed. Reportable errors could include:

A notice being made for a purpose, or for a type of data, which the public authority cannot seek;

Human error, such as incorrect transposition of information where communications data is acquired;

Disclosure of the wrong information by a CSP when complying with a notice;

Disclosure or acquisition of data in excess of that required.

- Recordable errors are ones where an error has occurred but has been identified before the communications data has been acquired. The Local Authority must keep a record of these occurrences, but a report does not have to be made to the IOCCO. Recordable errors could include:

A notice which is impossible for a CSP to comply with;

Failure to review information already held, e.g. seeking data already acquired or obtained for the same investigation, or data for which the requirement to obtain it is known to be no longer valid;

Notices being sent out to the wrong CSP;

Human error, such as incorrect transposition of information where communications data is not acquired;

Notices being sent out to CSP's that were not produced by the Designated Person who authorised the application.

8.80. Where a telephone number has been ported to another CSP then this does not constitute an error. Where excess data is disclosed, if the material is not relevant to the investigation it should be destroyed once the report has been made to the IOCCO. This should include destroying copies contained as attachments in emails. If having reviewed the excess material it is intended to make use of it, the Applicant must make an addendum to the original application to set out the reasons for needing to use this excess data. The Designated Person will then decide whether it is necessary and proportionate for the excess data to be used in the investigation. The requirements of DPA and its data protection principles must be adhered to in relation to an excess data.

8.81. Any reportable error must be reported to the Senior Responsible Officer and then to the IOCCO within five working days. The report must contain the unique reference number of the notice and details of the error, plus an explanation how the error occurred, indicating whether any unintended collateral intrusion has taken place and providing an indication of the steps that will take place to prevent a reoccurrence. The 'reporting an error by accredited SPoC form' (CD5) should be used for this purpose.

8.82. If the report relates to an error made by a CSP the Authority must still report it, but should also inform the CSP to enable them to investigate the cause.

8.83. The records kept for recordable errors must include details of the error, explain how the error occurred and provide an indication of the steps that will take place to prevent a reoccurrence. These records must be available for inspection by IOCCO inspectors and must be regularly reviewed by the Senior Responsible Officer.

8.84. The most common cause of errors is the incorrect transposition of telephone numbers, email addresses and IP addresses. In the vast majority of cases these addresses are derived from addresses available to the Applicant in electronic form. Therefore all Applicants are required to electronically copy communications addresses into applications when the source is in electronic form (for example forensic reports relating to mobile phones or call data records etc.) Communications addresses acquired from other sources must be properly checked to reduce the scope for error.

8.85. In circumstances where a reportable error is deemed to be of a serious nature, IOCCO may investigate the circumstances that led to the error and assess the impact of the interference on the rights of the affected person. IOCCO may inform the affected individual, who may make a complaint to the Investigatory Powers Tribunal. The Tribunal has full powers to investigate and decide any case within its jurisdiction which includes the acquisition and disclosure of communications data.

8.86. **SENIOR RESPONSIBLE OFFICER:** The Senior Responsible Officer is responsible for the following:

- The integrity of the processes of acquiring communications data;
- Compliance with the act and code of practice;
- Oversight of the reporting of errors to IOCCO;
- Engaging with IOCCO inspectors when they conduct inspections;
- Overseeing the implementation of any post-inspection action plans.

8.87. The Head of Paid Service is the Senior Responsible Officer with regard to the acquiring of communications data.

8.88. **CENTRAL RECORDS:** The Council must retain copies of all applications, authorisations, copies of notices and withdrawals of authorisations and cancellation of notices, cross-referenced against each associated document. This will be coordinated by the RIPA Coordination Officer who also holds copies of application for actual surveillance as per the Council's overarching RIPA policy. With the NAFN system, copies of the notices and authorisations are not routinely provided to the Designated Person, but print-offs of the completed online application forms will need to be provided to the RIPA Coordination Officer (consideration must be given to data sharing when dealing with internal investigations). Inspectors from the IOCCO will be able to obtain copies of all of these documents from NAFN.

8.89. The Senior Responsible Officer will have access to all of these forms as and when required.

8.90. The Local Authority must also keep a record of the following:

- Number of applications submitted to the NAFN SPOC;
- Number of applications submitted to the NAFN SPOC which were referred back to the applicant for amendment or declined by the SPOC;
- The reason for any amendments being required or application being declined by the SPOC;

- Number of applications that were approved by the Designated Person;
- Number of applications that were referred back to the applicant or rejected by the Designated Person;
- The reason for any referrals back or rejections;
- Number of notices requiring disclosure of communications data;
- Number of authorisations for conduct to acquire communications data;
- The priority grading of the application for communications data. The Council will only use Grade 3; matters that are routine but where appropriate will include specific or time-critical issues such as bail, Court dates etc;
- Whether any part of the application relates to a person who is member of a profession that handles privileged or otherwise confidential information (such as a medical doctor, lawyer, journalist, MP or minister of religion (and if so, which profession);
- Number of items of communications data sought for each notice or authorisation that was granted;

8.91. For each item of communications data included within a notice or authorisation the Local Authority must keep records of the following additional information:

- The Unique Reference Number of the application, notice and /or authorisation;
- The statutory purpose for which each item of communications data is being requested. The Council is only able to use the purpose of 'preventing or detecting crime or of preventing disorder';
- The type of crime being investigated;
- Whether the communications data is service use information (S21(4)(b) information) or subscriber information (S21(4)(c) information);
- The type of each item of communications data included in the notice or authorisation (such as fixed line telephone data, mobile telephone data or internet data);
- Whether each item of communications data relates to a victim, a witness, a complainant, a suspect, a next of kin, a vulnerable person or other person relevant to the investigation;
- The age of each item of communications data. (If the data includes more than one day, the age will be the oldest date of the data that is sought);
- Where the data sought is service use information on the total number of days of data being sought;
- The CSP from who the data is being acquired. All these records will need to be sent to IOCCO as requested.

8.92. The Lead Officer will keep a database of all applications, plus details of any notices and authorisations whether they are issued by the Local Authority or issued by NAFN on our behalf. This database will include records of any errors that have occurred. NAFN are able to provide on request statistical information about the numbers of notices or authorisations that they have issued.

9. INTERCEPTION OF COMMUNICATIONS COMMISSIONER'S OFFICE

9.1. The exercise of the powers and duties relating to communications data is kept under review by inspectors who work for the Interception of Communications

Commissioner's Office (IOCCO) under the control of the Interception of Communications Commissioner.

9.2. IOCCO state that if we receive a Freedom of Information request for a copy of our inspection report we should notify IOCCO, who will provide us with a suitably redacted version of the report to submit to the requester. No disclosure must take place until IOCCO has been consulted.

10. STRATEGY AND POLICY REVIEW

10.1. The Internal Audit Department will review and amend this policy as necessary to ensure that it continues to remain compliant and meets legislative requirements and the vision of the Council.

10.2. Responsible Officer: Head of Internal Audit.
Date: February 2016.

Review frequency as required by legislative changes / every three years.