Appendix B

Rotherham Metropolitan Borough Council

Acquisition & Disclosure of Communications Data

Under the Regulation of Investigatory Powers Act 2000 (RIPA)

June 2018

Rotherham Metropolitan Borough Council

Acquisition and Disclosure of Communication Data Policy

Rotherham Metropolitan Borough Council

Acquisition and Disclosure of Communication Data Policy

Introduction

What is Communications Data?

Communications data includes data such as itemised telephone call records and subscriber details. Communications data is not about giving access to the content of anybody's communications. For example, it is not about the contents of e-mails or interactions with websites. (Communications data includes Internet addresses, but only to the extent that they identify a network or a host computer, as opposed to a web page accessed by interacting with the host website).

Why is Communications Data useful?

Everyone needs to communicate in order to arrange their day to day activities, and criminals are no exception. Their need to communicate during the planning and execution of crime is a weakness which the authorities exploit, often with considerable success. Telephone call records, for example, provides a great deal of information on individuals' contacts and how they organise their life. This can be used in the planning of operations, the gathering of intelligence and, ultimately, it regularly assists in the prosecution of criminals.

Because the analysis of communications data can provide much information about the way in which people live their lives, this has led to concerns that the level of intrusion into an individual's privacy may be too great. The Government believes that there is a balance to be struck between the privacy of the individual and the needs of society as a whole to be protected from crime and other public safety risks.

Why introduce statutory provisions for access to communications data?

The Government introduced the access to communications data provisions in the Regulation of Investigatory Powers Act 2000 (RIPA) because it believed the regime surrounding access to communications data needed changing. In addition, there have been enormous changes in the telecommunications market. For example: the number of companies has grown; mass ownership of mobile phones; the emergence of totally new services; and Internet communications has grown dramatically. Public Authorities need to keep up with the changes in the communications marketplace; changes which criminals have been quick to exploit for their own purposes. Telephone call records, for example, can be of tremendous investigative value, and it is right that in certain circumstances public authorities should be able to access this material. However, it also involves a measure of intrusion into individual privacy and it is essential that access should be carefully controlled in accordance with European Convention on Human Rights (ECHR) proportionality requirements, authorisation only being given where necessary and justified for clearly defined statutory purposes. It is for these reasons that the Government established a statutory framework for access to communications data under RIPA and an associated Code of Practice.

Communications Data - RIPA Chapter II Part I

Chapter II Part I of RIPA provides that conduct other than interception (see s.21(I)) such as the acquisition and disclosure of communications data is lawful if authorised (see s.21(2)). Communications data is the 'who', 'when' and 'where' of a communication, but not the 'what' (i.e. the content of what was said or written). Communications data means any of the following:

(i) Traffic Data – this is information about a communication and the equipment used in transmitting it (e.g. information about the location of a mobile phone or an Internet Provider address allocation). **Local Authorities are not authorised to obtain access to traffic data.**

(ii) Service Use Information – this is information about the use a person makes of a postal or telecommunications service (e.g. itemized call records, records of connection to the internet or the timing and duration of usage).

(iii) Subscriber Information – this is information that communications service providers (CSPs) hold about people to whom they provide a service (e.g. names, addresses and telephone numbers).

For further guidance on the relevant communications please refer to the Code of Practice (paragraphs 2.12-2.35)

Lawful authority

The Act provides two different ways of permitting access to communications data; through an authorisation under section 22(3) and by a notice under section 22(4). An authorisation would allow the relevant public authority to collect or retrieve the data itself from the relevant CSP. A notice is given to a CSP and requires that operator to collect or retrieve the data and provide it to the public authority which served the notice. A designated person decides whether or not a notice or authorisation should be given.

Designated Persons in Local Authorities are Directors, Head of Service, Service Manager or equivalent. See the Regulation of Investigatory Powers (Communications Data) Order 2010, **SI 2010** No.480, I **Schedule 2, Part 2.**

Under section 22(2) of the Act, communications data may be sought if a designated person believes it is necessary for one or more of the following purposes (see s.21(2)):

- in the interests of national security;
- for the purpose of preventing or detecting crime or of preventing disorder;
- in the interests of the economic well being of the UK;
- in the interests of public safety;
- for the purpose of protecting public health;
- for the purpose of assessing or collecting any tax, duty, levy or other imposition, contribution or charge payable to a government department;
- for the purpose, in emergency, of preventing death or injury or any damage to a person's

physical or mental health, or mitigating the same:
- for any other purpose as specified by the Secretary of State.

However for our purposes, it is important to note that Local Authorities in England and Wales may authorise acquisition and disclosure of communications data only for the purpose of preventing or detecting crime or of preventing disorder.

It is important that all requests which the Council makes for Communications data, are properly made in accordance with this procedure. Failure to follow these procedures will leave the Council vulnerable to Court challenge and may mean that the Communications Data evidence acquired may not be admissible in Court proceedings

Authorisation Procedure

Acquisition of communications data under RIPA involves four roles.

- The Single Point of Contact
- The Applicant
- The Designated Person
- The Senior Responsible Officer

Single Point of Contact

All Local Authorities are now required to make all requests for communications data through a single point of contact (SPoC) at the National Anti-Fraud Network (NAFN). As such applicants within the local authority are required to consult a NAFN SPoC throughout the authorisation process, including before referring the case to a Designated Person for approval. The SPoC at NAFN will scrutinise the applications independently and provide advice to applicants and Designated Persons ensuring the local authority acts in an informed and lawful manner.

NAFN operates an electronic system whereby the Application is completed online by the investigating officer, this completed form is then forwarded electronically to the relevant Designated Person, and if the application is authorised then NAFN will return a copy to the Designated Person, who will liaise with Legal Services in respect making an application for Judicial Approval (see below). NAFN will advise whether an authorisation or notice is the most appropriate approach. If judicial approval is granted the NAFN SPoC will liaise with the appropriate CSP to acquire the relevant communications data. The results of the request will then be channeled through NAFN to the requesting officer.

The NAFN online system can be accessed by logging on to their website at www.NAFN.gov.uk. In order to access the system each applicant and Designated person will require log on details which are issued by NAFN. A user guide is available for operating the NAFN online system.

SPoCs should be in a position to:
- where appropriate, assess whether access to communications data is reasonably practical for the CSP:
- advise applicants and Designated Persons on the practicalities of accessing different types of communications data from CSPs:
- advise applicants and Designated Persons on whether communications data falls under

section 21(4)(a). (b) or (c) of the Act:
- provide safeguards for authentication:
- assess any cost and resource implications to both the public authority and the CSP.

Applications

The application form is subject to inspection by the Investigatory Powers Commissioner's Office ("IPCO") and both applicant and Designated Person may be required to justify their decisions. Applications to obtain communications data under the Act are made on a standard form. This is on the NAFN online system. This form is retained by the Council and NAFN and should contain the following minimum information:

- the name (or designation) and position of the officer requesting the communications data;
- the operation and person (if known) to which the requested data relates;
- a unique reference number and any operation name to which the application relates;
- a description, in as much detail as possible, of the communications data requested, specifying where relevant, any historic or future date(s) and, where appropriate, time period(s) (there will also be a need to identify whether it is communications data under section 21 (4)(b) or (c) of the Act);
- the reason why obtaining the requested data is considered to be necessary for one or more of the purposes in s.22(2) (the relevant purpose also needs to be identified);
- an explanation of why obtaining the data constitutes conduct proportionate to what it seeks to achieve;
- where appropriate, a consideration of collateral intrusion, the extent to which the privacy of others may be affected and why that intrusion is justified;
- consider and, where appropriate, describe any possible unintended consequences of the application; and
- the timescale within which the communications data is required. Where the timescale within which the material is required is any greater than routine, the reasoning for this to be included.

In addition to the above requirements, the degree of interference with an individual's rights and freedoms may be higher if the communications data being sought relates to a person who is a member of a profession that handles privileged or otherwise confidential information (including medical doctors, lawyers, journalists, Members of Parliament, or ministers of religion). It may also be possible to infer an issue of sensitivity from the fact that someone has regular contact with, for example, a lawyer or journalist. These situations do not preclude an application being made, but special consideration must be given to necessity and proportionality, including drawing attention to any such circumstances that might lead to an unusual degree of intrusion or infringement of rights and freedoms, particularly regarding privacy and, where it might be engaged, freedom of expression. Particular care needs to be taken by Designated Persons when considering such applications, including additional consideration of whether there might be unintended consequences of such applications and whether the public interest is best served by the application (see paragraphs 3.72 to 3.84 of the Code of Practice for further information).

The application form should subsequently record whether access to communications data was approved or denied, by whom and the date. Alternatively, the application form can be marked with a cross-reference to any authorisation granted or notice given (see paragraph 3.6 of the Code of Practice).

All applications relating to accessing communications data and associated documentation (renewals, cancellations etc) should be securely stored in files kept under lock and key when not in use.

Considerations for Designated Person

It is crucial that the Designated Person must be independent from operations and investigations when granting authorisations or giving notices related to those operations. Therefore, a Designated Person in a particular case should not be part of the same Council team who are carrying out the investigation (see paragraph 3.12 of the Code of Practice).

For an action to be necessary in a democratic society the access to communications data must pursue a legitimate aim as listed in s.23(2); and be proportionate to that aim.

Under section 22(5) of the Act, a designated person must also consider the conduct involved in obtaining the communications data to be proportionate. Proportionality is a crucial concept. In both the Act and the Code of Practice reference is made to the conduct being proportionate. This means that even if a particular case which interferes with a Convention right is aimed at pursuing a legitimate aim (as listed above) this will not justify the interference if the means used to achieve the aim are excessive in the circumstances. Any interference with a Convention right should be carefully designed to meet the objective in question and must not be arbitrary or unfair. Even taking all these considerations into account in a particular case, an interference may still not be justified because the impact on the individual or group is too severe.

A designated person needs to have in mind:

- the conduct which he is authorising or requiring in each case. In making a judgment as to proportionality, and also what the scope of the conduct is. For example, where the conduct covers the provision of ongoing communications data;
- where appropriate, where accessing the communications data is likely to result in collateral intrusion, whether the circumstances of the case still justify that access; and
- whether any urgent timescale is justified.

Judicial Approval

From 1st November 2013 it has been necessary to make an application to the Magistrates Court for Judicial Approval, in respect of all applications for Access to Communications Data.

A full procedural guide to making such an application for Judicial Approval is at Appendix 1 (this guide is applicable to applications for Directed Surveillance also). The Applicant and Designated Persons should liaise with Legal Services in respect of making an application for Judicial Approval, as a solicitor from Legal Services will make the application to Court and represent the Council at the hearing of the application.

Content of an Authorisation or Notice

A Designated Person will make a decision whether give an authorisation or to issue a notice based upon the application which is made. The application form is not served upon the CSP. Whether authorisation or a notice is granted, they must both be in writing, or if not, in a manner that

produces a record of it having been granted.
An authorisation must also:

- describe the conduct which is authorised and describe the communications data to be acquired, specifying, where relevant, any historic or future date(s) and, where appropriate, time period(s);
- specify the purpose for which the conduct is authorized, by reference to a statutory purpose under s 22(2) of RIPA;
- specify the office, rank or position held by the Designated Person granting the authorization. The Designated Person should also record their name (or designation) on any authorization they grant; and
- record the date and, when appropriate to do so, the time when the authorization as granted by the Designated Person.

If a notice is served upon a CSP it is in a standard format which must:

- specify the purpose for which the conduct is authorized, by reference to a statutory purpose under s 22(2) of RIPA;
- describe the communications data to be obtained or disclosed under the notice specifying, where relevant, any historic or future date(s) and, where appropriate, time period(s);
- include an explanation that compliance with the notice is a requirement of RIPA;
- specify the office, rank or position held by the Designated Person giving the notice. The name (or designation) of the Designated Person giving the notice should also be recorded;
- include a unique reference number and also identify the public authority;
- specify the manner in which the data should be disclosed. The notice should contain sufficient information including the contact details of the SPoC to enable the CSP to confirm the notice is authentic and lawful;
- record the date and, when appropriate to do so, the time when the notice was given by the Designated Person; and
- where appropriate, provide an indication of any urgency or time within which the CSP is requested to comply with the requirements of the notice.

The Senior Responsible Officer

The Senior Responsible Officer is responsible for;

- the integrity of the process in place to acquire communications data
- compliance with Chapter II of Part of RIPA and the Code of Practice
- oversight of reporting errors to IPCO (see below)
- engagement with the IPCO inspectors when they conduct inspections
- where necessary oversee the implementation of post-inspection action plans approved by the Commissioner

Within this Authority the SRO is the Assistant Director of Legal Services.

Duration of an Authorisation or Notice

Authorisations and notices will only be valid for a maximum of one month from when the

authorisation is granted or notice given. A designated person should specify a shorter period if that is satisfied by the request, since this may go to the proportionality requirements. For 'future" communications data disclosure may only be required of data obtained by the CSP within this period i.e. up to one month. For "historical" communications data disclosure may only be required of data in the possession of the CSP. A CSP should comply with a notice as soon as is reasonably practicable. Furthermore, they will not be required to supply data unless it is reasonably practicable to do so. (see paragraph 3.48 of the Code of Practice).

Renewal and Cancellation

Any valid authorisation or notice may be renewed for a period of up to one month by the grant of a further authorisation or the giving of a further notice.

A renewed notice takes effect at the point at which the notice it is renewing expires.

A Designated Person shall cancel a notice given under section 22(4) of the Act as soon as it is no longer *necessary,* or the conduct is no longer proportionate to what is sought to be achieved. The duty to cancel a notice falls on the designated person who issued it who should immediately liaise with the NAFN SPoC. The Designated Person must confirm the position in writing for the SPoC or, if not, in a manner that produces a record of the notice having been cancelled by the Designated Person. Where the Designated person who gave the notice to the CSP is no longer available, this duty should fall on a person who has temporarily or permanently taken over the role of the Designated Person.

(See paragraphs 3.45-58 of the Code of Practice).

Disclosure of Data

Notices under section 22(4) of the Act will only require the disclosure of data to:

- the person giving the notice i.e. the designated person; or
- another specified person. In practice, this is likely to be the SPoC.

Communications data, and all copies, extracts and summaries of it. must be handled and stored securely. In addition, the requirements of the Data Protection Act 1998 and its data protection principles should be adhered to (See Chapter 7 of the Code of Practice). In criminal proceedings, the principles under the Criminal Procedure and Investigations Act 1996 will need to be complied with (See paragraph 6.4 of the Code of Practice).

Retention of Data

Applications, and notices for communications data will be retained by NAFN until it has been inspected by the Commissioner. NAFN should also keep a record of the dates on which the notice is started, Judicial Approval is granted and the Notice is cancelled (See paragraph 6.1 of the Code of Practice).

Where any errors have occurred in the giving of notices, a record should be kept, and a report and explanation may a have to be sent to the Commissioner. An error can only occur after a Designated Person:

- has granted an authorization and the acquisition of date has been initiated; or
- has given notice and the notice has been served on a CSP in writing, electronically or orally.

Where an error occurs in the grant of an authorisation, the giving of a notice or as a consequence of any authorized conduct, or any conduct undertaken to comply with a notice, but the error is identified without data being acquired or disclosed wrongly, then a record should be kept.

Where an error results in communications date being acquired or disclosed wrongly, a report must be made to the Commissioner.
The practical arrangements for this Error reporting are as follows;

If there are any errors found with the data return (for example the wrong subscriber data) then the requesting officer must inform the Senior Responsible Officer and NAFN.

NAFN then contacts the SRO and reviews what has happened and why the error has occurred. It is the responsibility of the SRO to inform the IPCO and the appropriate CSP within 5 working days of the error being discovered. Where a reportable error is deemed to be of a serious nature, the Commissioner may investigate the circumstances that led to the error and assess the impact of the interference on the affected individual's rights. The affected individual may make a complaint to the Investigatory Powers Tribunal. Applications must also be retained to allow for the Tribunal to carry out its functions.
(See paragraphs 6.11 to 6.25 of the Code of Practice for more information on the recording and reporting of errors).

Oversight

IPCO oversees the use of powers for interception of communications, acquisition of communications data and the investigation of electronic data. As the authority uses NAFN as its SPOC, NAFN as opposed to the Council will be inspected on a regular basis. It is still important that all of the relevant documents are completed properly by the Council and stored appropriately. The operation of this policy shall be overseen by the Council's Audit Committee by receiving reports on a 6 monthly basis to ensure that the RIPA powers are being used consistently with this policy.

APPENDIX 1

GUIDE TO SEEKING MAGISTRATES' APPROVAL FOR RIPA SURVEILLANCE

Background

Chapter 2 of Part 2 of the Protection of Freedoms Act 2012 (sections 37 and 38) came into force on 1st November 2012. This changes the procedure for the authorisation of local authority surveillance under the Regulation for Investigatory Powers Act 2000 (RIPA).

From 1st November 2012 local authorities are required to obtain the approval of a Justice of the Peace (JP) for the use of any one of the three covert investigatory techniques available to them under RIPA namely Directed Surveillance, the deployment of a Covert Human Intelligence Source (CHIS) and accessing communications data.

An approval is also required if an authorisation to use such techniques is being renewed. In each case, the role of the JP is to ensure that the correct procedures have been followed and the relevant factors have been taken account of. There is no requirement for the JP to consider either cancellations or internal reviews.

Home Office Guidance

The Home Office has published guidance on the Magistrates' approval process both for local authorities and the Magistrates' Court:

http://www.homeoffice.gov.uk/publications/counter-terrorism/ripa-forms/local-authority-ripa-guidance/

This guidance is non-statutory but provides advice on how local authorities can best approach these changes in law and the new arrangements that need to be put in place to implement them effectively. It is supplementary to the legislation and to the two statutory Codes of Practice made under RIPA.

The New Magistrates' Approval Process

1. The first stage will be to apply for an authorisation in the usual way. Once this has been granted, the local authority will need to contact the local Magistrates' Court to arrange a hearing.

2. The hearing is a 'legal proceeding' and therefore local authority officers need to be formally designated to appear, be sworn in and present evidence or provide information as required by the JP. For the initial applications which are made following the requirement for Judicial Approval, Legal Services will attend at the Magistrates Court to present the application. In due course the Council may formally designate certain properly trained investigating officers for this purpose under section 223 of the Local Government Act 1972.

3. The Home Office suggests that the investigating officer will be best suited to making the application for Judicial Approval, although the Authorising Officer may also want to attend to answer any questions.

4. The local authority will provide the JP with a copy of the original RIPA authorisation. This forms the basis of the application to the JP and should contain all information that is relied upon. In addition, the local authority will provide the JP with two copies of a partially completed judicial application/order form (which is included in the Home Office Guidance)

5. The hearing will be in private and heard by a single JP who will read and consider the RIPA authorisation and the judicial application/order form. He/She may have questions to clarify points or require additional reassurance on particular matters. The forms and supporting papers must by themselves make the case. It is not sufficient for the local authority to provide oral evidence where this is not reflected or supported in the papers provided.

6. The JP will consider whether he or she is satisfied that, at the time the authorisation was granted or renewed, there were reasonable grounds for believing that the authorisation was necessary and proportionate. He/She will also consider whether there continues to be reasonable grounds. In addition the JP must be satisfied that the Authorising Officer was of an appropriate level within the local authority and that the authorisation was made in accordance with any applicable legal restrictions (e.g. meets the Serious Crime Test for Directed Surveillance)

7. The order section of the above mentioned form will be completed by the JP and will be the official record of the his/her decision. The local authority will need to retain a copy of the form after it has been signed by the JP.

Magistrate's Options

The JP may decide to –

- ***Approve the grant/renewal of the authorisation***

The grant/renewal of the authorisation will then take effect and the local authority may proceed to use the surveillance technique/acquisition of data technique mentioned therein. The surveillance/acquisition of data has to be commenced within one month of the Magistrates' Court approval.

- ***Refuse to approve the grant/renewal of the authorisation on a technicality***

The RIPA authorisation will not take effect and the local authority may <u>not</u> use the surveillance technique/acquisition of data technique in that case. The authority will need to consider the reasons for the refusal. A technical error in the form may be remedied without the need to go through the internal authorisation process again. The authority can then reapply for Magistrates' approval.

- ***Refuse to approve the grant/renewal and quash the authorisation***

A JP may refuse to approve the grant or renewal of an authorisation and decide to quash the original authorisation. This may be because he/she believes it is not necessary or proportionate. The RIPA authorisation will not take effect and the local authority may not use the surveillance technique/acquisition of data technique in that case. The JP must not exercise his/her power to quash the authorisation unless the local authority has had at least two business days from the date of the refusal in which to prepare and make further representations to the court.

Appeals

A local authority may only appeal a JP's decision to refuse approval of an authorisation, on a point of law by making an application for Judicial Review in the High Court.

The Investigatory Powers Tribunal (IPT) will continue to investigate complaints by individuals about the use of RIPA techniques by public bodies, including local authorities. If, following a complaint to them, the IPT finds fault with a RIPA authorisation it has the power to quash the JP's order which approved the grant or renewal of the authorisation. It can also award damages if it believes that an individual's human rights have been violated by the local authority.

Application for judicial approval for authorisation to obtain or disclose communications data, to use a covert human intelligence source or to conduct directed surveillance
Regulation of Investigatory Powers Act 2000 sections 23A, 23B, 32A, and 32B

Local authority:.....
Local authority department:.....
Offence under investigation[1]……...……
……...…
Address of premises or identity of subject:[2]……..……
……..

Covert technique requested: (tick one and specify details)

Communications Data	
Covert Human Intelligence Source	
Directed Surveillance	

Summary of details[3]

……
……
……
……
……
……
……

Note: this application should be read in conjunction with the attached RIPA authorisation/RIPA application or notice.

Investigating Officer .....

Authorising Officer .....

Officer(s) appearing before JP [4].....
Address of applicant department: .....
.....
Contact telephone number.....
Contact email address (optional) .....
Local authority reference.....
Number of pages.....

[5]Order made on an application for judicial approval for authorisation to obtain or disclose communications data, to use a covert human intelligence source or to conduct directed surveillance.
Regulation of Investigatory Powers Act 2000 sections 23A, 23B, 32A, 32B

Magistrates' court .....

Having considered the application, I (tick one):

☐ am satisfied that there are reasonable grounds for believing that the requirements of the Act were satisfied and remain satisfied, and that the relevant conditions are satisfied and I therefore approve the grant or renewal of the authorisation/notice.

☐ [6]refuse to approve the grant or renewal of the authorisation/notice.

☐ [7]refuse to approve the grant or renewal and quash the authorisation/notice.

Reasons .....……....

……..……

.....

Notes

.....

.....

Signed:

Date:

Time:

Full name:

Address of magistrates' court:

Notes to Assist Completion