

WEST WILTSHIRE DISTRICT COUNCIL

REGULATION OF INVESTIGATORY POWERS ACT 2000 (RIPA)

COMMUNICATIONS DATA PROCEDURE

1 Introduction

- 1.1 This procedure details the ways in which communications data may be requested and used by officers of this authority.
- 1.2 Part 1 Chapter 2 of the Regulation of Investigatory Powers Act 2000 (RIPA) deals with the acquisition and disclosure of communications data.
- 1.3 Communications data is information such as the name of a subscriber to a mobile phone, their address and the numbers called. It does not include the content of any emails, telephone calls, letters etc.
- 1.4 The Act allows the Council to require communications data (not the contents) only where it is necessary for **preventing or detecting crime or preventing disorder**.
- 1.5 Acquiring communications data must be authorised to have the legal protection of RIPA from potential Human Rights Act (Article 6 and 8) breaches.
- 1.6 **Communications data which has been acquired unlawfully, could result in costs being awarded against the Council. Officers and all external agencies employed by West Wiltshire DC must comply with RIPA and this procedure. Failure to comply with this procedure may result in disciplinary action in line with the Council's policy.**
- 1.7 RIPA allows a specific number of Council officers to gain access to communications data; this includes service use data and subscriber data. These are defined in section 2 below.
- 1.8 The Government has appointed the Interception of Communications Commissioner to oversee the legislation and, as a Local Authority, we can be audited on our acquisition of communications data at any time. In addition, the Investigatory Powers Tribunal has been established to hear any complaints from aggrieved persons on the Council's conduct in this area.

2 Definitions

- 2.1 **Communications data** includes information relating to the use of:
 - a telecommunications system (mobile phone, land line, email, fax and internet)
 - postal service (anything written on the outside)

It is NOT the contents on the communications or emails.

There are three categories of communications data.

- 2.2 **Traffic data [RIPA section 21 (4) (a)] – the Council cannot acquire this type of information which:**
 - Identifies the sender or recipient of a communication
 - Identifies the location of a communication
 - Web browsing information
 - Appears on the outside of a postal item
 - Online tracking of communications

- 2.3 **Service use information which the council can acquire [RIPA section 21 (4) (b)]** - includes
- Itemised telephone call records
 - Itemised connection records
 - Itemised times and duration of calls and connections
 - Information on the connection, disconnection and reconnection of services
 - Information on the use of forwarding/redirection services (by post or telecommunications service providers)
 - Records of postal items such as registered, recorded and special delivery postal items

- 2.4 **Subscriber information which the council can acquire [RIPA section 21 (4) (c)]** - includes
- Subscriber information such as who is the subscriber of phone number 01234 567890 or who is the subscriber of email account xyz@xyz.anyisp.co.uk
 - Subscribers' account information, including payment methods
 - Addresses for installation and billing

- 2.5 **Communication Service Providers (CSP)** include
- Telecommunications providers
 - Internet service providers
 - Postal services

3 Access to communications data

- 3.1 There are two ways in which officers can access communications data which is required for the preventing or detecting crime or preventing disorder. These are by:
- an authorisation, and
 - a notice

- 3.2 **Authorisation** - This method is used where West Wiltshire staff will be accessing or retrieving data themselves without the CSP being asked to provide the communications data. It is unlikely that the council will use this method of accessing data.

- 3.3 **Notice** - A notice under RIPA section 22 (4) is used where a CSP may be in the possession of data or be able to obtain the relevant data.

4 Procedure for obtaining a notice

- 4.1 A notice may be served on a CSP to obtain data or for the CSP to disclose all the data in its possession or subsequently obtained by it.
- 4.2 Before a notice can be served, the investigating officer must complete an application for the communications data.
- 4.3 The format of the application can be found in Appendix A to this procedure.
- 4.4 The investigating officer must complete sections 1 to 14 of the form. The statutory grounds for making the application to obtain the data will be for the preventing or detecting crime or preventing disorder (section 22 (2) (b)).

- 4.5 The three key issues which the application must consider are:
- Necessity
 - Proportionality
 - Collateral intrusion
- 4.6 Once completed the form will be passed to the Single Point of Contact (SPoC). The SPoC is a postholder accredited by the Home Office to check the forms, ensure compliance with the codes of practice and provide assurance to the Designated Persons that the notice is lawful and free from errors. The SPoC is currently the Environmental Health Service Manager.
- 4.7 The SPoC must check the form and complete sections 15 and 16. They can either reject the application or pass it to a Designated Person for authorising and signing.
- 4.8 The Designated Person (DP) is an equivalent role to that of the authorising officer under the surveillance part of RIPA. The DP is responsible for granting the application.

They must consider if the application is:

- necessary on the grounds specified, and
- proportionate

They must also assess any collateral intrusion which may arise due to the disclosure of the communications data.

- 4.9 If satisfied that the application meets the above criteria they shall complete section 17 of the form and return it to the SPoC.
- 4.10 The service managers permitted to authorise data communications requests (Designated Person) are:
- Revenues and Benefits Service Manager
 - Head of Human Resources & Customer Services
 - Development Control Manager
- 4.11 On receiving an approved application form the SPoC shall complete a Section 22 (4) notice contained in Appendix B to this procedure.
- 4.12 The notice shall be sent to the relevant CSP and the legislation gives them 10 working days to respond to the request for the data.
- 4.13 To find out which CSP provides the service two website are useful. These are open sources of information at:
- www.magsys.co.uk
www.ukphoneinfo.com

Entering a partial phone number will identify which CSP provides the mobile service.

5 Senior Responsible Person

- 5.1 The Senior Responsible Person is responsible for the:
- Integrity of the process
 - Compliance with the Act and Code
 - Oversight of reporting of errors, their cause and solutions

5.2 The Senior Responsible Person is currently the Head of Legal and Democratic Services.

6 Benefits of compliance

6.1 Compliance with Part 1 Chapter 2 of RIPA guarantees that the acquisition of communications data is lawful for all purposes. It also ensures that we respect the rights of our residents to privacy under the Human Rights Act.

- they know their actions are lawful; and
- the Council is safe from legal action.

7 Recording and filing applications for authorisations and notices

7.1 The SPoC must ensure that the documents are centrally recorded. Any officer who applies for communications data must forward the documents to the SPoC (Environmental Health Service Manager) as soon as is reasonably practicable.

7.2 The SPoC will keep a register of all authorisation documents (in the file which contains the surveillance authorisations). All applications must be allocated a unique reference number.

7.3 The RIPA procedures shall be reviewed every two years in co-ordination with the biannual review of the corporate enforcement policy.

8 Duration of Notices and Authorisations

8.1 Authorisations and notices last for 1 month.

8.2 They must clearly state their start and end times

9 Renewal of Notices and Authorisations

9.1 If the notice or authorisation needs to be renewed, the investigating officer must add a paragraph to the end of the application form assessing the necessity and proportionality for an extension.

9.2 The revised form must then be handed to the SPoC and if considered satisfactory signed again by the Designated Person.

10 Cancellation of notices and authorisations

10.1 All notices and authorisations must be cancelled when it is no longer necessary or proportionate.

10.2 The SPoC or Designated Person shall inform the CSP of any cancellation.

11 Home Office guidance

11.1 Further detailed guidance can be found on the Home office web site <http://security.homeoffice.gov.uk/ripa/communications-data> and in the code of practice on the acquisition and disclosure of communications data.

Appendix A

Chapter II of Part I of the Regulation of Investigatory Powers Act 2000 (RIPA)

Application for Communications Data

This form is to obtain authorisation to issue a RIPA Section 22 Notice to a CSP to release Communications Data

Name of Public Authority making this application: West Wiltshire District Council

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

7) Operation Name (if applicable)		8) STATUTORY PURPOSE
		Preventing or detecting crime or of preventing disorder

9) COMMUNICATIONS DATA

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

10) NECESSITY

State why it is necessary in relation to your investigation or operation to obtain this data for the purpose listed at question 8)

What do you expect to achieve from obtaining the communications data? Explain why you have requested the specific date/time period. If applicable, explain the time scale within which the data is required to be delivered to you.

11) PROPORTIONALITY

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

Why does the intrusion benefit the investigation or operation you are undertaking? When considering the benefits to the investigation or operation, can the level of intrusion be justified against the individual's right to privacy?

--

12) COLLATERAL INTRUSION

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

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

--

13) TIMESCALE

Identify and explain the timescale within which the data is required

--	--

14) APPLICANT

I undertake to inform the SPoC of any change in circumstances that no longer justifies the acquisition of the data

Applicant's Signature		Date	
------------------------------	--	-------------	--

15) ASSESSMENT BY ACCREDITED SPoC.

If the request is NOT reasonably practical for the CSP explain why	
Specify which sub-section the data falls within	Click here for options: -
State whether notice or authorisation is appropriate	Click here for options: -
Describe any adverse cost or resource implications to either your public authority or the CSP?	
If the request will provide any excessive data to that requested by the applicant, give details.	
Are there other factors the DP should be aware of?	
Name of Accredited SPoC	

16) AUTHORISATION (Completed by Accredited SPoC when appropriate)

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

- CSP is not capable of obtaining or disclosing the communications data;
- The investigation or operation may be prejudiced if the CSP is required to obtain or disclose the data;
- There is an agreement in place between the public authority and the CSP relating to the appropriate mechanisms for the disclosure of the data;
- The designated person considers there is a requirement to conduct a telephone subscriber check but a CSP has yet to be conclusively determined as the holder of the communications data.

Describe the communications data to be acquired specifying, where relevant, any historic or future date and/or time periods sought. Also, describe the course of conduct required to obtain it.
Name of the relevant CSP

The statutory purpose for which the conduct may be authorised is set out at section 8 of this form.
The office, rank or position of the designated person should be recorded within section 17 of this form.
A record of the date & time the granting of an authorisation is made should be recorded within section 17 of this form

17. DESIGNATED PERSON

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

*If you, based on this application, **believe** acquiring the communications data is necessary for one of the purposes within section 22(2) of the Act consider the following:*

- Why do you **believe** the conduct involved in obtaining the data is proportionate to the objective(s)? In making that judgement you should take in consideration any additional information from the SPoC.*
- Where accessing the communication data is likely to result in meaningful degree of collateral intrusion, why you **believe** the request remains justified and proportionate to the objective(s)?*

My considerations in approving / not approving this application are:

- I authorise the conduct to be undertaken by the SPoC as set out in section 16 of this form.
- I give Notice and require the SPoC to serve it on (insert name of CSP) . The Notice bears the unique reference number

Name		Office, Rank or Position	
Signature		Time and Date	

Appendix B

NOTICE - Section 22(4) of the Regulation of Investigatory Powers Act 2000 (RIPA)

This form is sent to the CSP to request Communications Data

Where it appears to the designated person that a CSP is or may be in possession of, or be capable of obtaining, any communications data, the designated person may, by notice require the CSP -

(a) if the CSP is not already in possession of the data, to obtain the data; and

(b) in any case, to disclose all of the data in his possession or subsequently obtained by him.

S. 22(6) - It is the duty of the CSP to comply with any notice given to him under subsection (4).

Name of Public Authority making this application **West Wiltshire District Council**

Other SPoC Reference*		Unique Reference Number of Notice	
Details of the CSP		Name of the CSP Address of CSP For attention of	
Statutory Purpose	S22 (2)(b) Prevention and detection of crime		
Designated Person Giving Notice	Name of the DP Office, rank or position Date Notice given and if appropriate the time		
This Notice is valid for one month when given by the Designated Person			
Describe the communications data to be acquired specifying, where relevant, any historic or future date and/or time periods sought.	Data applied for Time period (if applicable)		
DCG Grade 3 – SPoC may indicate any specific or critical time issues such as bail dates, court dates, persons in police custody, specific line of investigation in serious crime (S.81(2) RIPA) investigation <u>and</u> the acquisition of data will <u>directly assist</u> in the prevention or detection of the crime. URGENT (DCG Grade 1 or 2) may only be initiated by SPoC and may require liaison with CSP staff.	Grade 3: If, and only if there is a specific or critical time issue state the 'target date' for the disclosure of the data Explain the reason for the setting of a target data Reminder: Ordinarily all Notices are Grade 3 and will be dealt with in date order when received by the CSP. DCG has requested the IOCCO Inspectors to make appropriate comment on the use of the grading scheme during their inspections of law enforcement agencies URGENT delivery of data Click here for options:-		
Specify the manner in which the data should be disclosed	Click here for options:-		
SPoC Office Contact Details and Address	TEL FAX EMAIL POSTAL Name of Accredited SPoC Mob TEL Reminder: If you have requested a "24/7" response from the CSP make sure you supply sufficient contact details so		
If there is a specific or critical time issue indicated or the matter is DCG Grade 1 or 2 URGENT then the Accredited SPoC details MUST be completed			

	that you and your SPoC colleagues can be easily contacted
Date Notice served	and if appropriate the time

Application process for communications data

APPENDIX C

