BUCKINGHAMSHIRE COUNTY COUNCIL

www.buckscc.gov.uk

Acquisition and Disclosure

Of Communications Data

Policy

REGULATION OF INVESTIGATORY POWERS ACT 2000 – PART 1 CHAPTER 11

TABLE OF CONTENTS

ACQUISITION AND DISCLOSURE OF COMMUNICATIONS DATA

1. There are circumstances in which it will be necessary in order to prevent or detect crime or prevent disorder for Council officers to investigate the use by individuals under investigation of telecommunications. Such investigations are likely to be a prima facie interference with the subject's right to private life under ECHR Article 8. However, they can be justified where they are undertaken in a manner prescribed by law and are necessary and proportionate to achieving a legitimate aim such as the prevention or detection of crime or the prevention of disorder. Chapter II of Part I of the *Regulation of Investigatory Powers Act 2000* ("RIPA") provides the framework under which the Council's officers must operate if their investigations require the acquisition or disclosure of communications data.

2. **Communications Data** relates to transactions involving:

   - The Postal Service
   - Emails
   - Internet
   - Fixed line phone calls
   - Mobile phone calls

3. The Council cannot intercept private communications in order to discover their contents. There are circumstances in which Council officers can record communications e.g. telephone communications where either the sender or the receiver consents but this would constitute covert surveillance and authorisation would be required under the relevant provisions of RIPA (see the Council's policy on covert surveillance).

4. There are also circumstances in which Council officers can obtain access to certain classes of "communications data". This is summarised in the table below:

RIPA TERM	**MEANING**	**EXAMPLE**	**CAN THE COUNCIL'S OFFICERS SEEK TO ACQUISITION OR DISCLOSURE**
Subscriber Data	Information about the person who subscribes to or uses the communications service	Name and address of user of a phone number	Yes
Service Use Data	Information about the use made of the communication service	Telephone numbers called and duration of calls	Yes
Traffic Data	Information about how the communication was transmitted	Location of a mobile phone when communication was sent	No

The Council's Officers can only seek the acquisition or disclosure of Subscriber Data and Service Use Data.

5. Communications data is generated, held or obtained by Communications Service Providers (CSPs) in the course of providing communications services.

Roles and Responsibilities

6. Before considering the authorisation process, a brief note is required on the terminology of the different roles.

7. The applicant or Investigating Officer is the Council officer conducting an investigation and wishing to acquire communications data.

8. The **Designated Person** is a Council officer of a sufficient rank to grant an authorisation or notice for the acquisition of communications data. The decision whether to grant an authorisation or notice is ultimately a decision for a Designated Person.

9. A **Single Point of Contact** is a Council officer (or officers) with the appropriate Home Office accredited training to provide objective advice and assistance to the applicant and the Designated Person. The SPoC will act as a conduit for communications between the Council and a CSP. Although termed a "Single" PoC there are in fact several SPoCs within the Council. Where reference is made to consulting a SPoC, the applicant officer should approach the SPoC within their area of operations e.g. Trading Standards, Planning & Environment or Legal who is likely best to be able to advise on the practicalities of their investigation.

10. The **Senior Responsible Officer** is responsible for ensuring that the Council complies with RIPA and the Codes of Practice; for overseeing the reporting of errors to the Commissioner; and for identifying the causes of any errors and implementing processes to minimise the likelihood of their repetition.

11. A Designated Person may also be a SPoC. Where that is the case, the same person can play both roles in the process set out below (so e.g. there will be no need to send the application to a SPoC before submitting it to a Designated Person who is him or herself a SPoC).

12. The Designated Persons, Single Points of Contact and Senior Responsible Officer are set out in Appendix A attached Communications Personnel List. The Senior Responsible Officer will ensure that the Personnel List is revised as and when necessary.

How can I obtain communications data?

13. There are two means by which an Investigating Officer might seek to acquire communications data. First, the Investigating Officer might apply for a notice to be served on the CSP requiring the CSP to collect and retrieve the data and provide it to the Council. This is the usual type of application that will be made at the Council.

14. Second, the Investigating Officer might apply for an authorisation to extract the required communications data from records held by a CSP. The communications data would be extracted by a SPoC. An authorisation may be appropriate where:
- the CSP is unable to obtain or disclose the communications data; or
- the Council has agreed mechanisms with a CSP relating to appropriate mechanisms for disclosing communications data; or
- where the CSP has yet to be identified; or
- giving notice to the CSP would prejudice the investigation.

The Authorisation Process

15. In addition to this Guidance, the Authorisation Process is set out in the Flow Chart, which forms Appendix B.

16. Before making an application, the Investigating Officer should discuss the proposed application with their line manager and if possible should discuss the proposed application with the SPoC before completing and submitting a formal application. The SPoC should be able to advise on whether an application is appropriate and what sort of application is appropriate.

17. In following the authorisation process, it should be noted that there is no need to print off hard copies, obtain wet signatures and send documents through the internal post. Electronic signatures will suffice providing the emails are retained and they capture all conduct and activity to create a full audit trail.

18. The officer making the application must use the Communications Data Application Form available at http://security.homeoffice.gov.uk/ripa/publication-search/ripa-forms/communications-data.doc. (Current version as at 2009 appears as CD1 in Appendix C). Guidance Notes are also available at that location. The Form requires the officer to:

- include the name and the office, rank or position held by the person making the application
- include a unique reference number
- include the operation name (if applicable) to which the application relates
- specify the purpose for which the data is required (in the Council's case this must be the prevention or detection of crime or the prevention of disorder)
- describe the communications data required specifying where relevant any historic or future dates and, where appropriate, time periods

- explain why the acquisition of that data is considered necessary and proportionate to what is sought to be achieved by acquiring it
- consider and describe any meaningful collateral intrusion and any steps that can be taken to minimise such intrusion
- identify and explain the time scale within which the data is required

19. In explaining why the acquisition of data is necessary and proportionate to the particular aim there should be a short explanation of the crime, the suspect, the victim or witness and the phone and how these are linked together. In the proportionality section, the Investigating Officer should outline the data which is being sought, its relevance to the investigation and the specific objective to be achieved. It may be appropriate to highlight any strategic objectives e.g. if the action is being taken as part of a drive against a particular type of crime. If there is likely to be collateral intrusion, the Investigating Officer should indicate how it will be managed.

To whom do I submit the application?

20. The application should first be submitted to the SPoC. The SPoC must consider whether the application is practical; advise on what approach to take if data involves more than one CSP; assess cost and resource implications to the Council and the CSP; and keep appropriate records of any conversations with the Designated Person. The SPoC must ensure that a full log is kept for each application. It is ultimately for the SPoC to identify the CSP and produce a draft Notice.

21. If satisfied that the application is justified, the SPoC should send the application to the Designated Person. As noted above, the same person can be both the SPoC and the Designated Person. The final decision whether to grant the application lies with the Designated Person.

22. If the SPoC is not satisfied that an application is justified or if the SPoC identifies defects with the application, the application should be returned with reasons and specific advice.

23. Each application should be logged on the database held by Legal Services.

Urgent applications

24. In exceptional circumstances, an authorisation or notice may be given orally. This would be appropriate only where:

    - there is an immediate threat to life such that a person's life may be endangered if the normal application procedure were required
    - there is an exceptionally urgent operational requirement (within 48 hours) whereby the acquisition of communications data will directly assist the prevention or detection of the commission of a serious offence (i.e. an offence that can result in more than 3 years imprisonment)

25. These circumstances are unlikely to arise in relation to the matters dealt with by the Council but if they do arise, and if authorisation is granted or notice given, the conduct authorised should be undertaken or the notice served on the CSP as soon as practicable.

26. In the case of an oral notice, retrospective written notice must be given to the CSP within one working day of the oral notice being given.

27. As soon as possible after the grant of the authorisation or notice, the Investigating Officer must complete a retrospective application including an explanation of why the matter was urgent and the Designated Person must make a record of the grant of authorisation or notice and the time at which the grant was made.

The decision on the application

28. The Designated Person must believe that the conduct required by the authorisation or notice is necessary and proportionate to the aim in the circumstances. The Designated Person must consider all the circumstances and in particular:

- whether there is any alternative means of obtaining the information
- the extent of any intrusiveness into the privacy of the individual subject to investigation
- the likelihood and extent of any intrusiveness into the privacy of individuals who are not subject to the investigation ("**collateral intrusion**")

29. The Designated Person must record in writing the reasons for granting or refusing the application. The reasons recorded must be sufficient to indicate that the Designated Person has properly considered the individual application. Tailoring the comments to the individual application is the best means of demonstrating that it has been given proper consideration.

30. Where the Designated Person refuses an application, the Designated Person should keep a copy of the application, which should be returned to the applicant with a statement of the reasons for refusing the application.

31. Where a notice is given, the Notice must be in writing (unless it is urgent) and:

- contain enough information to allow the CSP to comply with the requirements of the notice
- include a unique reference number and identify the public authority
- specify the purpose for which the notice has been given (the prevention or detection of crime or the prevention of disorder)
- describe the communications data to be obtained or disclosed specifying, where relevant, any historic or future dates and, where appropriate, time periods
- explain that compliance with the Notice is a required by RIPA

- specify the name and officer, rank or position of the Designated Person giving the notice
- specify the manner in which data should be disclosed. The notice should include the contact details of the SPoC to enable a CSP to confirm that the notice is authentic and lawful
- record the date and, where appropriate, time when the notice was given by the Designated Person
- where appropriate, the notice should provide an indication of any urgency or time within which the CSP is requested to comply with the requirements of the notice

32. The Notice must be on Notice Form, available at http://security.homeoffice.gov.uk/ripa/publication-search/ripa-forms/ripa-section-22-notice-update (Current version as at 2009 appears as CD2 in Appendix C).

Serving the Notice/Acquiring the Communications Data

33. The Designated Person should forward the authorised Notice to the SPoC who should forward the Notice to the CSP.

34. The SPoC must ensure that any Notice does not purport to require a CSP to do anything that it is not reasonably practicable for the CSP to do. The Notice may only require a CSP to disclose the communications data to a Designated Person or to the SPoC. Normally, the CSP should disclose the communications data not later than ten working days from the date the Notice is served on the CSP. However, where the Designated Person determines that the CSP could not comply within ten days, the Designated Person shall indicate a longer period up to a period of one month from the date Notice is given.

35. Where an authorisation is given, the Authorisation must be in writing (unless it is urgent) and must:

- describe the conduct which is authorised and the communications data to be acquired, specifying any relevant time period
- specify the purpose for which the conduct is authorised (the prevention or detection of crime and the prevention of disorder)
- specify the name and the office, rank or position held by the Designated Person
- record the date and, in time critical circumstances, the time when the authorisation was granted.

36. The Designated Person must send the completed application to the SPoC who should acquire the communications data in the appropriate manner.

37. The original copy of any communications data received, known as the “golden copy” should be securely stored and a copy sent to the applicant. If the necessary, the golden copy may subsequently be adduced in evidence on production of a witness statement from the CSP concerned.

Renewals and Cancellation

38. Authorisations and Notices are valid for one month from the date on which the Authorisation is granted or Notice given.

39. All Authorisations and Notices should refer to communications data for a specific date or period which should be clearly indicated.

40. Where an Authorisation or Notice relates to the acquisition of specific data that may be generated in future, the future period is restricted to no more than one month from the date on which the Authorisation was granted or Notice given.

41. An Authorisation or Notice may be renewed for a period of up to one month from the date the Authorisation or Notice would otherwise expire.

42. The Investigating Officer must clearly set out the reasons for seeking a renewal.

43. The Designated Person must consider whether it is necessary and proportionate to renew the Authorisation or Notice. If the Designated Person decides to renew, the date and, when appropriate, the time of the renewal should be noted and the reason clearly stated. The Designated Person should carefully consider the length of any renewal and should carefully consider the length of the period for which data is required; the greater the period the greater the burden on the CSP and so the stronger the reason would have to be.

44. If the Designated Person considers that a renewal would not be appropriate, this should be recorded and the reasons stated.

45. If, at any time after granting an Authorisation, the Designated Person decides that the Authorisation is no longer necessary or proportionate to the aims pursued, the Designated Person must withdraw the Authorisation.

46. If, at a time after giving Notice to a CSP but before the CSP has provided the data requested, the Designated Person decides that it is no longer necessary for the CSP to act on the Notice or that it would no longer be proportionate, the Designated Person must cancel the Notice.

47. The Designated Person or the SPoC must then notify the CSP that the Notice has been cancelled.

Disclosure & Retention of Data

48. In the case of a Notice, the CSP will provide the communications data to the SPoC. The SPoC must determine whether the data provided fulfils the requirements of the Notice.

49. In the case of an Authorisation, the CSP will acquire the data and determine whether the data acquired fulfils the authorisation.

50. Communications data acquired under RIPA, together with all copies, extracts and summaries, must be handled and stored securely. In addition, the requirements of the DDA 1998 must be adhered to.

Record Keeping

Inspection Records

51. Applications, Authorisations, copies of Notices, withdrawals, cancellations and renewals must be retained in written or electronic form and physically attached or cross-referenced where they are associated with each other.

52. The SPoC will hold original copies. Copies will also be held by the applicant and copies will be provided to Legal Services. Legal Services will maintain a database in relation to communications data.

53. These records must be made available for annual inspection by the Interception of Communications Commissioner.

Annual Return

54. The Senior Responsible Officer must keep a record of:

- the number of applications submitted to a Designated Person for grant of an Authorisation or Notice
- the number of Authorisations granted
- the number of Notices granted
- the number of urgent applications processed

55. This record must be sent annually to the Interception of Communications Commissioner.

Errors

56. The proper application of the Council's policy should minimise errors as far as possible. However, errors may still occur. This section applies to errors that occur after a Designated Person has granted an authorisation and the acquisition of data has been instigated or after notice has been given and served on a CSP

57. Where an error has occurred but is only identified after communications data has been acquired or disclosed, the SPoC should complete the Communications Data Error Form available at http://security.homeoffice.gov.uk/ripa/publication-search/ripa-forms/reporting-public-authority-error?view=Binary including: (Current version as at 2009 appears in CD3 in Appendix C).

- details of the error
- an explanation of how the error occurred
- indications of whether any unintended collateral intrusion has taken place
- indications of what steps have been, or will be, taken to ensure that similar error does not reoccur.

58. The details must be submitted to and will be retained by Legal Services and the Senior Responsible Officer must be informed.

59. The Senior Responsible Officer must report all "reportable errors" to the Commissioner. Such errors are errors where communications data is acquired or disclosed wrongly:

- an authorisation or notice made for a purpose or for a type of data (e.g. traffic data) the Council cannot seek
- human error such as incorrect transposition of information from an application to an authorisation or notice
- disclosure of the wrong data by a CSP when complying with a notice
- acquisition of the wrong data by the Council when engaging in conduct specified in an authorisation

60. The Senior Responsible Person must keep a record of all "recordable errors". Recordable errors include:

- a notice given which is impossible for a CSP to comply with
- failure to review information already held e.g. unnecessarily seeking data already acquired or obtained
- failure to serve written notice on a CSP within one working day of urgent oral notice being given or urgent oral authorisation granted

Data Protection Safeguards

61. Communications data and all copies, extracts or summaries of it must be handled and stored securely. The requirements of the Data Protection Act 1998 and its data protection principles must be adhered to.

62. It should be noted that an individual may make a Subject Access Request under the Data Protection Act to a CSP for information about whether they have been subject to a notice to disclose communications data. However, a CSP could refuse such a request where it would be likely to prejudice the prevention and detection of crime or the apprehension or prosecution of offenders.

63. Where a CSP is unsure about whether disclosure of the fact of a notice would be likely to prejudice an investigation or operation, the SPoC should be able to advise them. If a request is made to the SPoC for advice, the SPoC must be sure to respond in good time to enable a response to the subject access request.

64. Communications data acquired under RIPA should be detained for only so long as necessary. Communications data should be disposed of in accordance with the Criminal Procedures and Investigations Act 1996.

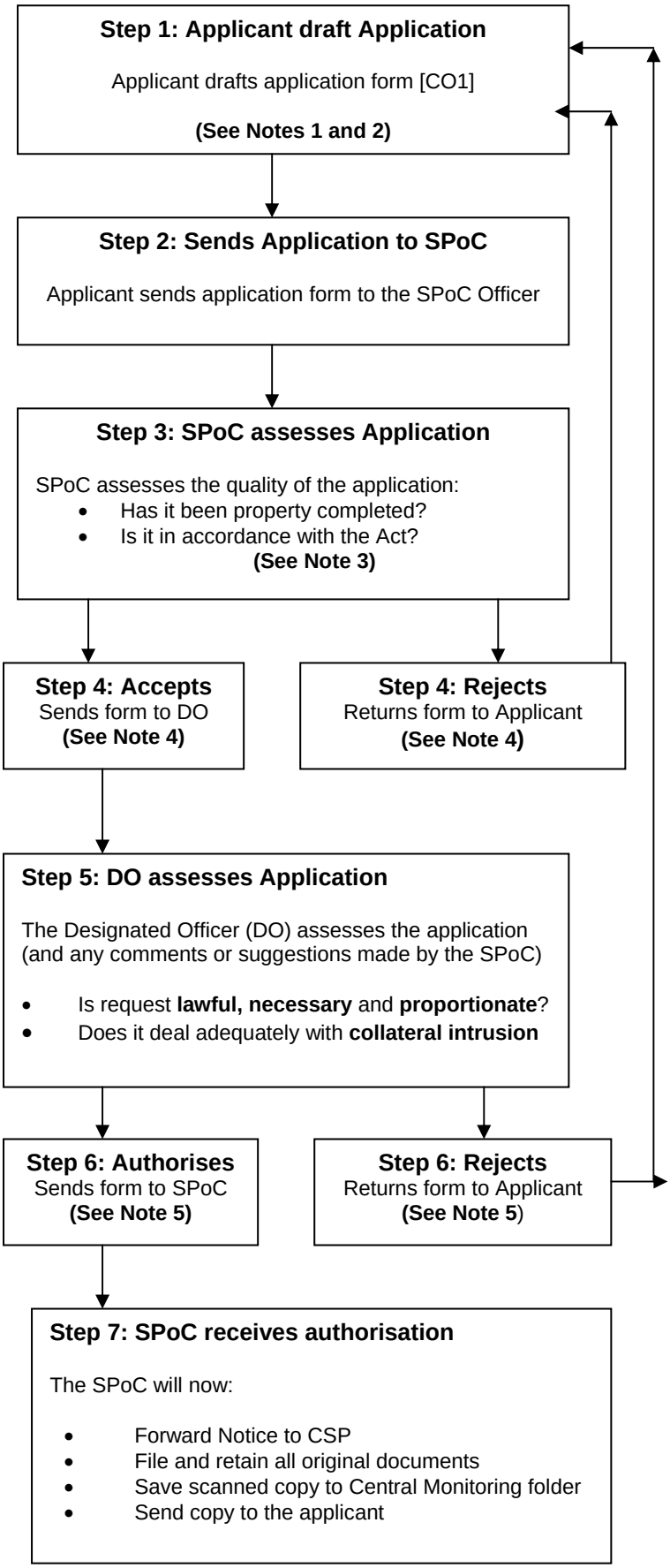
APPENDIX A

COMMUNICATIONS PERSONNEL LIST

ROLE	NAME	JOB TITLE	DEPARTMENT
SENIOR RESPONSIBLE OFFICER	ANNE DAVIES	HEAD OF LEGAL AND DEMOCRATIC SERVICES	LEGAL AND DEMOCRATIC SERVICES
DESIGNATED PERSON / SPOC	YVONNE GIBSON	GROUP SOLICITOR	LEGAL AND DEMOCRATIC SERVICES
DESIGNATED PERSON / SPOC / ACCREDITED OFFICER	TERRY CARTER	ASSISTANT HEAD OF TRADING STANDARDS	TRADING STANDARDS
DESIGNATED PERSON / SPOC / ACCREDITED OFFICER	AMANDA POOLE	ASSISTANT HEAD OF TRADING STANDARDS	TRADING STANDARDS
SPOC	DAVID SUTHERLAND	WASTE REDUCTION MANAGER	PLANNING & ENVIRONMENT
RIPA CO-ORDINATOR	HELEN FULLARTON	PA TO YVONNE GIBSON	LEGAL AND DEMOCRATIC SERVICES

APPENDIX B

FLOWCHART OF APPLICATION PROCESS



Note 1
Applicant should discuss proposed application with line manager to find alternative options for obtaining the information required.

Applicant may also wish to discuss content, scope and aims of the application and type of application with the SPoC before submitting the application

Note 2
The application should include:
- The purpose for which the data is required
- The nature of the enquiry
- Details of the data required
- The timescale in which the data is needed
- A statement clearly setting out:
  1. why request is necessary
  2. why request is proportionate
  3. steps to be taken to minimise collateral intrusion

Note 3
The SPoC will:
- Asses practicability and cost/resource implications of granting the request
- Keep appropriate records of any conversations with the Designated Officer

Note 4
If the SPoC accepts that the application is justified and reasonably practicable, s/he:
- Will send the application form to the DO for signing off
- May include any appropriate additional information/comments for consideration by DO

If the SPoC rejects the application, s/he will:
- Return the application to the applicant
- Specify in writing reason(s) for rejection
- Save a copy of rejected application + reason(s) to the Council's Central Monitoring Records

Note 5
If DO authorises the application, s/he will:
- Sign and send form to the SPoC
- Document any discussions conducted in reaching the decision

If DO rejects the application, s/he will:
- Return the application to the applicant
- Specify in writing reason(s) for rejection
- Save a copy of rejected application + reason(s) to the Council's Central Monitoring Records

KEY

Applicant:	Officer making the application
DO:	Designated Officer who authorises the Application
SPoC:	Single Point of Contact between BCC and CSP
CSP:	Communications Services Provider

APPENDIX C

LIST OF FORMS IN USE FOR COMMUNICATIONS DATA REQUESTS

Form CD1: Communications Data Application

Form CD2: Communications Data Notice

Form CD3: Communications Data Error Report