APPENDIX 2

CHESHIRE EAST COUNCIL

ACQUISITION AND DISCLOSURE OF COMMUNICATIONS DATA UNDER THE REGULATION OF INVESTIGATORY POWERS ACT 2000 (RIPA)

POLICY AND PROCEDURE

This document sets out the requirements for gaining authorisation to acquire communications data under RIPA

ACQUISITION AND DISCLOSURE OF COMMUNICATIONS DATA UNDER THE REGULATION OF INVESTIGATORY POWERS ACT 2000 (RIPA)

POLICY

P1 BACKGROUND

P1.1 The Regulation of Investigatory Powers Act 2000 (RIPA) came into effect in September 2000. It establishes a regulatory framework for the acquisition of communications data by setting up an authorisation procedure. Communications data are defined in Section 21(4) of RIPA and include information held by any postal service or telecommunications service or system. RIPA seeks to ensure that public authorities only acquire communications data where it is necessary for a specific, legally prescribed purpose, and that the acquisition is carried out in such a way that the risk of infringing the rights of individuals is kept to an absolute minimum.

P1.2 The acquisition of communications data may interfere with Article 8 of the Human Rights Act 1998 which provides that everyone has the right to respect for his private and family life, his home and correspondence. This right is subject to an important qualification - Paragraph 2 of Article 8 provides that:

"There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others."

P1.3 RIPA therefore protects an individual's rights and freedoms that are guaranteed by the European Convention and given further effect by the Human Rights Act 1998, whilst allowing a public authority to carry out certain, necessary covert surveillance activity.

P2 INTRODUCTION

P2.1 Cheshire East Council will on occasion need to acquire communications data in order to carry out its enforcement functions effectively. Examples of enforcement activities which may require the acquisition of communications data include, in particular, trading standards investigations relating to doorstep crime, counterfeiting and other fraudulent trading activity. **A local authority may only acquire communications data for the purpose of the prevention or detection of crime or the prevention of disorder.**

P2.2 The acquisition of communications data by a public authority is likely to constitute an infringement of an individual's rights and freedoms which are protected by the Human Rights Act 1998. However, by following the authorisation procedures set out by RIPA, officers of the Council are ensuring that they can demonstrate that the data acquisition is for a purpose permitted by the Human Rights Act

1998 and that it is a proportionate measure to take, given all of the circumstances. Compliance with RIPA will significantly reduce the likelihood of any acquisition of communications data by the Council being unlawful and therefore subject to legal challenge.

P3 CHESHIRE EAST COUNCIL'S POLICY IN ACCORDANCE WITH RIPA AND THE HOME OFFICE CODE OF PRACTICE ON THE ACQUISITION AND DISCLOSURE OF COMMUNICATIONS DATA

P3.1 The purpose of this policy and its associated procedure is to reinforce the requirements of RIPA and the Code of Practice, to ensure compliance with RIPA, to protect the rights of individuals and to minimise the risk of legal challenge as a result of officer actions.

P3.2 The Council is fully committed to complying with the Human Rights Act 1998 and RIPA. In order to ensure compliance, all communications data acquisition must be carried out in accordance with the legislative framework and the Council's RIPA policy and procedure.

P3.3 In particular, any legislative restrictions on the type of communications data that a local authority is authorised to access must be observed; any acquisition of data must be properly authorised and recorded; the tests of necessity and proportionality must be satisfied; and the potential for collateral intrusion must be considered and minimised. Definitions of terms are included in the RIPA procedure.

P3.4 Any officer intending to acquire communications data will only do so if the evidence or intelligence sought cannot be obtained by other means.

P3.5 Acquiring communications data without authorisation or outside the scope of the authorisation will not only mean that the "protective umbrella" of RIPA is unavailable but may result in disciplinary action being taken against the officer/officers involved. RIPA also established an independent Tribunal (the Investigatory Powers Tribunal) that has full powers to investigate and decide any case within its jurisdiction that includes the acquisition and disclosure of communications data.

P3.6 The Council's Acquisition and Disclosure of Communications Data Policy and Procedure will be reviewed every year, or sooner if necessary (e.g. in the event of legislation being amended or revoked).

4 APPLICATION

4.1 The Council's policy is operational forthwith and applies to all Council staff employed under a permanent, temporary, fixed term or casual contract. It also applies to any contractors and/or subcontractors employed by the Council to undertake activities covered by this policy and procedure. All relevant Council contracts issued to contractors/subcontractors will include a term that this policy and associated procedures are to be observed when operating on behalf of the Council.

4.2 A copy of this policy document will be made available for public inspection at the Council offices' reception areas and on the Council's website.

ACQUISITION AND DISCLOSURE OF COMMUNICATIONS DATA UNDER THE REGULATION OF INVESTIGATORY POWERS ACT 2000 (RIPA)

PROCEDURE

1 CATEGORIES OF COMMUNICATIONS DATA

1.1 Section 21(4) of RIPA defines three categories of communications data, only two of which can be accessed by the local authority.

1.2 Local authorities are **not** authorised to acquire "traffic data" i.e. information that identifies any person, equipment or location to or from which a communication is or may be transmitted. Furthermore, the powers do **not** extend to the acquisition of the contents of the communication itself.

1.2.1 The categories of communications data which may be acquired by the local authority are:

- section 21(4)(b) of RIPA: any information (excluding traffic data and the contents of a communication) about the use made by any person (i) of any postal service or telecommunications service; or (ii) in connection with the provision to or use by any person of any telecommunications service, or any part of a telecommunication system, and
- section 21(4)(c) of RIPA: any information (excluding traffic data, the contents of a communication and information falling within paragraph section 21(4) (b) of RIPA) that is held or obtained, in relation to persons to whom he provides the service, by a person providing a postal service or telecommunications service .

1.2.2 Examples of the information that may be obtained under section 21(4) (b) of RIPA are listed below. The full list appears in the Code of Practice for the Acquisition and Disclosure of Communications Data.

- Itemised telephone call records
- Itemised records of connections to internet services
- Itemised timing and duration of service usage (calls and/or connections)
- Information about amounts of data downloaded and/or uploaded
- Records of postal items, such as records of registered post, recorded or special delivery postal items, records of parcel consignment, delivery and collection.

1.2.3 Examples of the information that may be obtained under section 21(4) (c) of RIPA are listed below. The full list appears in the Code of Practice.

- Subscriber checks (also known as “reverse look ups”)

- Subscriber or account holders’ account information, including names and addresses for installation, and billing including payment method(s), details of payments

- Information about the subscriber to a PO Box number.

- Information about apparatus used by or made available to, the subscriber or account holder including the manufacturer, model, serial number and apparatus codes.

2 ORGANISATIONS FROM WHICH LOCAL AUTHORITIES MAY ACQUIRE COMMUNICATIONS DATA

2.1 All communications data are acquired from Communication Service Providers (CSPs). These may be:

- Telecommunications service providers (e.g. mobile phone service providers, landline phone service providers or International Simple Voice Resellers)

- Internet service providers (e.g. internet service providers (ISPs), Virtual ISPs and Portals)

- Postal service providers

3 OFFICERS ABLE TO GRANT AUTHORISATIONS

3.1 Under section 22(2) of RIPA an authorisation for the acquisition of communications data may be granted or a notice issued by a Designated Person where he believes that the conduct is:

<u>Necessary</u> in the circumstances of a particular case:

- for the purpose of preventing or detecting crime or of preventing disorder, and

<u>Proportionate</u> to what it seeks to achieve.

3.2 Detecting crime includes establishing by whom, for what purpose, by what means and generally in what circumstances any crime was committed, the gathering of evidence for use in any legal proceedings and the apprehension of the person (or persons) by whom any crime was committed.

3.3 The Regulation of Investigatory Powers (Communications Data) Order 2010 (SI 2010/480) prescribes the office, rank or position of a Designated Person within a local authority as the Director, Head of Service, Service Manager or equivalent.

4 THE TESTS OF NECESSITY AND PROPORTIONALITY

4.1 The acquisition of communications data should only be authorised if the Designated Person is satisfied that:

- **The action is NECESSARY (in a democratic society) on the following grounds:**
  - For the prevention or detection of crime or the prevention of disorder
- **The surveillance is PROPORTIONATE - The Human Rights Act defines a measure or action as proportionate if it:**
  - Impairs as little as possible the rights and freedoms (of the individual concerned and of innocent third parties),
  - Is carefully designed to meet the objectives in question is not arbitrary, unfair or based on irrational considerations.

5 COLLATERAL INTRUSION

5.1 The Designated Person must also take into account the risk of intrusion into the privacy of persons other than those who are directly the subject of the investigation or operation. This is termed “collateral intrusion”.

5.2 Any application should include an assessment of the risk of any collateral intrusion and what steps can reasonably be taken to avoid this (if any). This should be a factor taken into account by the Designated Person when considering the proportionality of the acquisition of the communications data.

5.3 The Designated Person should be informed if the acquisition of the data unexpectedly infringes the privacy of any individual not under investigation. Consideration should then be given to determine whether it is necessary to report an error, or whether the authorisation should be amended and re-authorised, or whether a new authorisation is required. It should be noted that there is not likely to be any collateral intrusion identified when acquiring subscriber data.

6 ROLE AND RESPONSIBILITIES OF THE SINGLE POINT OF CONTACT (SPoC)

6.1 Integral to the acquisition of communications data under RIPA is the Single Point of Contact (‘SPoC’). The Home Office Code of Practice recommends that all authorities that use powers to acquire communications data have a SPoC, which may be an individual Accredited Officer or a unit comprised of more than one Accredited Officer.

6.2 All Accredited Officers must attend a Home Office Approved Course and, on successful completion of an examination, will be added to the Home Office list of Accredited Officers. In addition, the Accredited Officer must keep abreast of the law relating to, and developments within, the communications industry.

6.3 The SPoC appointed by the Council has the following responsibilities:

- To assess whether access to communications data in a particular case is reasonably practical for the Communication Service Providers (CSPs)

- To advise investigators and designated persons on the practicalities of accessing different types of communications data from different Communication Service Providers (CSPs)

- To advise investigators and Designated Persons on whether specific communications data falls under Section 21(4) (b) or 21(4) (c) of RIPA

- To assess any cost and resource implications for both the Council and the CSP

- To provide a safeguard for CSPs that authorisations and notices are authentic

- To retain records of all applications, authorisations and notices

- To retain a record of the dates on which authorisations and notices are started and cancelled

- To retain all applications in the event that there may be a Complaints Tribunal

- To retain a record of any errors that may have occurred in the granting of authorisations, or issuing of notices, and provide an explanation to the Interception of Communications Commissioner

- To maintain a SPoC log sheet for each application they are involved in.

6.4 The SPoC will assess the application and in particular whether the request has been made properly and whether the required communications data can reasonably be obtained together with any adverse cost or resource implications. Following this assessment, the SPoC must forward a copy of the application for consideration by the Designated Person for signature.

6.5 This SPoC system aims to provide an efficient regime, as it ensures consistency in dealing with the postal or telecommunications operators on a regular basis, enables the Council to self-regulate, and reduces the burden on the postal and telecommunications operator. It also provides a guardian and gatekeeper function to ensure that the Council acts in an informed and lawful manner.

7 THE SENIOR RESPONSIBLE OFFICER

7.1 The Borough Solicitor has been designated as the Senior Responsible Officer and will be responsible for:

- the integrity of the process to acquire the communications data,
- compliance with Chapter II of Part 1 of the Act and the Code of Practice for the Acquisition and Disclosure of Communications Data,

- oversight of errors, the implementation of processes to minimise errors and engagement with inspectors of the Interception of Communications Commissioner's Office (IOCCO) during inspections, and
- where necessary, oversight of the implementation of post-inspection action plans approved by the Commissioner.

8 INFORMATION TO BE PROVIDED IN APPLICATIONS FOR THE ACQUISITION OF COMMUNICATIONS DATA

8.1 All applications to acquire communications data must be made in writing by the applicant/investigating officer on the appropriate form. Officers should ensure that only current forms are used, obtained from the Home Office website (http://security.homeoffice.gov.uk/ripa/).

8.2 All such requests must include the following information:

- Name or designation of the officer requesting the communications data
- The operation and person (if known) to which the requested data relates
- A description of the data requested and, where appropriate, the relevant time period(s)* (*see 9.5 below)
- The category of communication data by reference to the relevant section of RIPA
- The grounds on which the acquisition of the data is considered to be necessary
- An explanation as to why the acquisition of the data is considered proportionate to what it seeks to achieve
- An indication (where appropriate) that the matter of collateral intrusion has been considered
- The timescale within which the data is required.

9 PROCEDURE FOR ACQUIRING COMMUNICATIONS DATA

9.1 The Act provides two alternative means for acquiring communications data by way of:

- authorisation under section 22(3), or
- a notice under section 22(4).

9.2 Completed application forms should be initially assessed by the SPoC. If it appears to the SPoC that the application reaches the legal threshold for the acquisition of communications data, he/she must then give the application form a unique

reference number, identify the relevant Communications Service Provider (CSP) and insert the CSP's details on the application before passing it to the Designated Person for consideration.

9.3 If the SPoC does not consider that the application reaches the legal threshold, he must return the application for further development and record this on a log sheet which must be retained. The SPoC should ensure that only the current form is used, obtained from the Home Office website http://security.homeoffice.gov.uk/ripa/).

9.4 The Designated Person will assess all applications forwarded by the SPoC and either authorise or reject the applications. If the application is refused, the SPoC will return a copy of the application with the reason for rejection and note this on the log sheet.

9.5 If a Notice is required under section 21(4)(b), this must be drafted by the SPoC and submitted to the Designated Person with the application. The Designated Person must then insert their name and the date and time of issue (which must be the same time and date as the approval of the application). The SPoC will then serve the notice on the CSP. The SPoC should ensure that only current forms are used, obtained from the Home Office website (http://security.homeoffice.gov.uk/ripa/).

9.5 The notice should be retained by the SPoC must be in writing or, if not, recorded in such a manner that produces a record, and must include:

- A unique reference number and the name of the Local Authority
- A description of the data to be obtained or disclosed specifying where relevant, any historic or future date(s) and where appropriate, time periods,
- The purpose for which the data is required under s. 22(2) (the prevention or detection of crime or prevention of disorder)
- The name (or designation) and office, rank or position of the Designated Person
- A record of the date and when appropriate the time when the notice was given by the Designated Person
- The manner in which the data should be disclosed. The notice should include the name and contact details of the SPoC.
- If relevant, any indication of urgency or time within which the CSP is requested to comply.
- An explanation that compliance with the notice is a requirement of the Act.

9.6 The SPoC should have particular regard to the period of time for which data are requested and specify the shortest period in which the objective for which the data are sought can be achieved. To do otherwise would have an impact on the proportionality requirement and impose an unnecessary burden on the CSP.

9.7 The Designated Person can grant an authorisation under s. 22(3) instead of giving a notice. The s. 22(3) authorisation will enable the SPoC to engage in conduct to acquire data under s. 21(4)(c) to identify the user of a phone or communications address. The SPoC has one month from the authorisation being granted to engage in the conduct. This reduces the bureaucracy previously experienced with number porting and secondly enables the SPoC, where necessary, to apply for additional account information in order to identify the user of an unregistered prepaid mobile telephone, without referring each request back to the Designated Person.

9.8 An authorisation must be granted in writing or, if not, in a manner that produces a record of it having been granted and must:

- Describe the conduct which is authorised and describe the communications data to be acquired by that conduct specifying, where relevant, any historic or future date(s) and, where appropriate, time periods;

- Specify the purpose for which the conduct is authorised, by reference to a statutory purpose under section 22(2) of the Act;

- Specify the name (or designation) and office, rank or position of the Designated Person; and

- Record of the date and when appropriate the time when the notice was given by the Designated Person

9.9 In the vast majority of cases, communications data will be acquired via an assurance that authorisation has been given or via a notice. At present the Council does not have direct access to service provider systems in order to be able to retrieve communications data direct by prior agreement between the local authority and the relevant service provider.

10 DURATION OF AUTHORISATIONS AND NOTICES

10.1 All notices and authorisations requesting communications data from the service provider are valid for a one month from the date on which the authorisation is granted or notice given.

11 RENEWALS

11.1 Notices and authorisations can 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 authorisation or notice takes effect upon the expiry of the authorisation or notice it is renewing.

11.2 Where the Designated Person agrees to the renewal, the Designated Person must have considered the reasons why it is necessary and proportionate to continue, and record the date of the renewal.

12 CANCELLATIONS

12.1 The Designated Person should cancel a notice if at any time after giving the notice 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 primarily on the Designated Person who issued it, or on that person's behalf, by the SPoC. The SPoC should ensure that only the current form is used, obtained from the Home Office website (http://security.homeoffice.gov.uk/ripa/).

12.2 In the event of the cancellation of a notice, the SPoC must inform the relevant postal or telecommunications operator of the cancellation without delay.

12.3 A record of cancellation must be recorded on the appropriate form by the SPoC and retained

12.4 Similarly, where the Designated Person considers that an authorisation should cease to have effect, because the conduct authorised becomes unnecessary or no longer proportionate to what was sought to be achieved, the authorisation should be withdrawn.

13 RECORDS

13.1 Applications, authorisations copies of notices and records of the withdrawal and the cancellation of notices must be retained in written or electronic form and physically attached or cross-referenced where they are associated with each other.

13.2 All records must be held centrally by the SPoC and be available for inspection by a representative of the Interception of Communications Commissioner's Office.

14 ERRORS

14.1 When a reportable error (i.e. where communications data is acquired or disclosed wrongly) has been made by the local authority, the matter should be reported to the Senior Responsible Officer and then in written or electronic form to the Interception of Communications Commissioner's Office. In deciding if an error is reportable, the local authority should refer to the Code of Practice.

14.2 In cases where an error has occurred but is identified by the local authority or the CSP without data being acquired or disclosed wrongly (a 'recordable error') a record will be kept. These records will be available for inspection by the Commissioner.

15 SCRUTINY

15.1 The Borough Solicitor will ensure that an annual report is submitted to the Council's Audit and Governance Committee. The report will include details of the overall number and type of authorisations granted and the outcome of the case, where known. In addition, the report will provide a breakdown of the same information by service or groups of services, as appropriate.

15.2 The report should also include the results of the most recent inspection carried out by a representative of the Communications Commissioner's Office, where applicable (inspections may not take place annually).

16 FURTHER INFORMATION

16.1 For further guidance please see the relevant Home Office guidance available from the Home Office website http://www.homeoffice.gov.uk/ or contact Legal Services.