Annex B

HUNTINGDONSHIRE DISTRICT COUNCIL

ACQUISITION OF COMMUNICATIONS DATA

REGULATION OF INVESTIGATORY POWERS ACT 2000
(PART I, CHAPTER II)

POLICY & PROCEDURE

CONTENTS

INTRODUCTION

The powers provided by the Regulation of Investigatory Powers Act 2000 (RIPA) allow the Council to obtain Communications Data to progress Criminal Investigations from Communications Service Providers (CSP's). It is not to be confused with the Councils Monitoring at Work Policy and Practices under the Lawful Business Practices Legislation. This latter legislation relates to the monitoring of the Council's own communication and computer systems.

Part 1 of RIPA introduces a statutory framework to regulate the access to communications data by public authorities consistent with the Human Rights Act 1998. All applications for Communications Data will be made through one of the Council's Accredited Officers known as Single Point of Contacts (SPoC's) who have passed a Home Office approved course. These Officers are based in the Councils Fraud Team located at Pathfinder House. One centrally held record will be maintained by the SPoC's to prevent duplication of acquiring communications data. This will also assist with the councils responsibilities with regard to record keeping.

This Policy sets out the Councils procedures and approach to obtaining and handling Communications Data for the purposes of preventing or detecting crime or of preventing disorder. It should be read in conjunction with the Home Office Interception of Communications Data Code of Practice (the codes) which explains the duties and responsibilities placed upon each party involved in these processes and creates a system of safeguards, consistent with the requirements of article 8 of the ECHR http://www.homeoffice.gov.uk/publications/counter-terrorism/ripa-forms/interception-comms-code-practice . This policy will be reviewed periodically.

The Codes can be obtained from the Home Office Website and are available to all Council staff involved in the acquisition of Communications Data.

Both this policy and the Codes of Practice will be followed at all times and under no circumstances should unauthorised access to obtain Communications Data be sought outside of this guidance or by requiring, or inviting, any postal or telecommunications operator to disclose communications data by exercising any exemption to the principle of non-disclosure of communications data under the Data Protection Act 1998 ('the DPA').

The Codes of Practice are admissible in evidence in criminal and civil proceedings.

A Communications Service Provider (CSP's) is an operator who provides a postal or telecommunications service such as Royal Mail and the usual Telephone Service providers as well as Internet Service Providers.

What is Communications Data

Communications Data does not include the contents of any communication. It is not lawfully possible for Council employees under any circumstances to obtain the contents of communications. SPoC/Accredited officers will ensure they are aware and remain up to date with the less obvious communications data which would constitute contents such as email headers.

The term 'communications data' embraces the 'who', 'when' and 'where' of a communication but not the content, not what was said or written. It includes the manner in which, and by what method, a person or machine communicates with another person or machine. It excludes what they say or what data they pass on within a communication including text, audio and video (with the exception of traffic data to establish another communication such as that created from the use of calling cards, redirection services, or in the commission of 'dial through' fraud and other crimes where data is passed on to activate communications equipment in order to obtain communications services fraudulently).

Consultation with the Council's Single Point of Contact (SPoC) will determine the most appropriate plan for acquiring data where the provision of a communication service engages a number of providers. It may be advisable that applicants seek advice and guidance when where enquiries regarding communications data are being considered within an investigation.

Types of Communications Data

There are three types of Communications Data which may be obtained dependant upon what the legislation allows the Public Authority to lawfully acquire. They are:

(a) Traffic Data

(b) Service Use Information

(c) Subscriber/ Account information

Huntingdonshire District Council has no lawful authority to obtain Traffic Data. However it can lawfully obtain Service Use data and Subscriber/Account information if the application meets the test of Necessity and Proportionality which will be decided by the Designated Person (Authorising Officer).

Traffic Data

The Act defines certain communications data as 'traffic data' in sections 21(4)(a) and 21(6) of the Act. This is data that is or has been comprised in or attached to a communication for the purpose of transmitting the communication and which 'in relation to any communication':

Examples of traffic data, within the definition in section 21(6), include:

- information tracing the origin or destination of a communication that is, or has been, in transmission (including incoming call records);

- information identifying the location of equipment when a communication is, has been or may be made or received (such as the location of a mobile phone);

- information identifying the sender or recipient (including copy recipients) of a communication from data comprised in or attached to the communication;

- routing information identifying equipment through which a communication is or has been transmitted (for example, dynamic IP address allocation, file transfer logs and e-mail headers – to the extent that content of a communication, such as the subject line of an e-mail, is not disclosed);

- web browsing information to the extent that only a host machine, server, domain name or IP address is disclosed;

- anything, such as addresses or markings, written on the outside of a postal item (such as a letter, packet or parcel) that is in transmission and which shows the item's postal routing;

- record of correspondence checks comprising details of traffic data from postal items in transmission to a specific address, and

- online tracking of communications (including postal items and parcels).

Any message written on the outside of a postal item, which is in transmission, may be content (depending on the author of the message) and fall within the scope of the provisions for interception of communications for which Council has no Authority to obtain. For example, a message written by the sender will be content but a message written by a postal worker concerning the delivery of the postal item will not. All information on the outside of a postal item concerning its postal routing, for example the address of the recipient, the sender and the post-mark, is traffic data within section 21(4)(a) of the Act.
*Huntingdonshire District Council has no lawful authority to obtain Traffic Data***.**

Service Use Information

Data relating to the use made by any person of a postal or telecommunications service, or any part of it, is widely known as 'service use information' and falls within section 21(4)(b) of the Act and the Council can lawfully obtain this data..

Examples of data within the definition at section 21(4)(b) include:

- itemised telephone call records (numbers called);

- 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;
- information about the use made of services which the user is allocated or has subscribed to (or may have subscribed to) including conference calling, call messaging, call waiting and call barring telecommunications services;
- information about the use of forwarding/redirection services;
- information about selection of preferential numbers or discount calls;
- records of postal items, such as records of registered post, recorded or special delivery postal items, records of parcel consignment, delivery and collection.

Subscriber Information

The third type of communication data, widely known as 'subscriber information', is set out in section 21(4)(c) of the Act. This relates to information held or obtained by a CSP about persons to whom the CSP provides or has provided a communications service. Those persons will include people who are subscribers to a communications service without necessarily using that service and persons who use a communications service without necessarily subscribing to it, and the Council can lawfully obtain this data

Person includes any organisation and any association or combination of persons.

Examples of data within the definition at section 21(4) (c) include:

- ‘subscriber checks’ (also known as ‘reverse look ups’) such as “who is the subscriber of phone number 012 345 6789?”, “who is the account holder of e-mail account example@example.co.uk?” or “who is entitled to post to web space *www.example.co.uk*?”;

- information about the subscriber to a PO Box number or a Postage Paid Impression used on bulk mailings;

- information about the provision to a subscriber or account holder of forwarding/redirection services, including delivery and forwarding addresses;

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

- information about the connection, disconnection and reconnection of services to which the subscriber or account holder is allocated or has subscribed to (or may have subscribed to) including conference calling, call messaging, call waiting and call barring telecommunications services;

- information about apparatus used by, or made available to, the subscriber or account holder, including the manufacturer, model, serial numbers and apparatus codes;

- information provided by a subscriber or account holder to a CSP, such as demographic information or sign-up data (to the extent that information, such as a password, giving access to the content of any stored communications is not disclosed.

The SPoC will provide advice and assistance with regard to the types of Communications Data which can be lawfully obtained and how that data may assist with an investigation.

Who Can We Obtain the Data From and For What reason?

Communications data can be obtained from a Communications Service Provider (CSP's) A CSP is an operator who provides a postal or telecommunications service such as Royal Mail and the usual Telephone Service providers. However there may be less obvious companies which may be classed as a CSP and advice should be sought from the SPoC.

Council can only process and consider applications to access Communications Data from within this Authority. Under no circumstances will applications be accepted for outside authorities/agencies. However, it may be necessary during joint investigations to obtain Communications Data. If this becomes necessary it is important that we are not bending the rules and applying or using the data where we would not normally be allowed to either access the data or that the other organisation has no lawful power to obtain Communications Data.

Lawful Reason to Access Communications Data

The Council's only lawful reason to access Communications Data is for

- the purpose of preventing or detecting crime or of preventing disorder;

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.

Using Other Powers

The codes state where a public authority seeks to obtain communications data using provisions providing explicitly for the obtaining of communications data (other than Chapter II of Part I of the Act) or using statutory powers conferred by a warrant or order issued by a person holding judicial office, the SPoC should be engaged in the process of obtaining the data to ensure effective co-operation between the public authority and the CSP.

Although there is some limited provision for obtaining some low grade Communications Data by other Statutory means such as The Social Security Administration Act the position of this Council is that the RIPA legislation will be used.

Should it be necessary to obtain Communications Data via other means such as a court order or should data be required from a CSP which falls outside of the definition of Communications Data the application should be handled by a SPoC.

The Two Ways of Obtaining Communications Data

The legislation provides two different methods of acquiring communications data (see below). The SPoC will provide advice regarding the method to be used and complete the relevant form.

The two methods

- an Authorisation under section 22(3), or
- a Notice under section 22(4).

An Authorisation (see Authorisation Form) should be used to obtain all section 21(4)(c) data (see page 8) unless it is being requested from the same provider as the inextricably linked service use data under section 21(4)(b) such as itemised billing. Both would normally be requested using a Notice in these circumstances. It will be the role of the SPoC to determine which method should be used. Unless using an automated system the Authorisation will be forwarded to the CSP by the SPoC.

Note

Although this is the advice of the Home Office, some CSPs state that they require a notice for data which is not obtained from their automated system. The SPoC will determine the correct method to be used.

Notices and Authorisations

A Notice and Authorisation are documents which when authorised and approved by a Justice of the Peace are forwarded to the CSP by the SPoC. Both are virtually identical documents requesting the CSP to provide the data which would usually be returned to the SPoC. However, a Notice is a Legal document which the CSP has to comply with. The decision of a designated

person whether to give a Notice or Authorisation shall be based upon information presented to them in an application form.

Ordinarily the CSP should disclose, in writing or electronically, the communications data to which a Notice or an authorisation relates not later than the end of the period of ten working days from the date the Notice is served upon the CSP. Should the data not be returned within this period they should only be contacted by the SPoC.

The original Authorisation or Notice will be retained by the SPoC within the public authority

Duration of Authorisations and Notices

As from 1 November 2012 there is a requirement for authorisations and notices to be approved by a Justice of the Peace (JP). From the date that the authorisation or notice is approved by the JP, (which follows its authorisation by the DP), it has a validity of a maximum of one month. This means the conduct authorised should have been commenced or the notice served within that month.

Realistically there should be no significant delay between the application being approved by the JP and the request to obtain the data.

A month means a period of time extending from a date in one calendar month to the date one day before the corresponding or nearest date in the following month. For example, a month beginning on 7 June ends on 6 July, a month beginning on 30 January ends on 28 February or 29 February in a leap year.

Internal Investigations

The Codes state where an investigation relates to an allegation of criminal conduct by a member of a public authority, that public authority (or another public authority appointed to investigate the complaint) may use their powers under Part 1 Chapter II to obtain communications data for the purpose of preventing and detecting the alleged or suspected crime where the investigating officer intends the matter to be subject of a prosecution within a criminal court. Should it be determined there are insufficient grounds to continue the investigation or insufficient evidence to initiate a prosecution within a criminal court, it will, with immediate effect, no longer be appropriate to obtain communications data under the Act.

If Communications Data is sought in connection with internal staff committing crimes against the Council it is important that the enquiry is a genuine Criminal Investigation with a view to proceeding Criminally as opposed to just a Disciplinary matter.

Advice may be required from the Councils Legal section if this arises.

Roles of Staff Involved in the Process

Acquisition of communications data under the Act involves four roles within a relevant public authority. A list of the Officers who have authority to act for Huntingdonshire District Council in these matters is attached in **ANNEX A**.

The Applicant

The applicant is a person involved in conducting an investigation or operation who makes an application in writing for the acquisition of communications data. The applicant completes an application form, setting out for consideration by the designated person, the necessity and proportionality of a specific requirement for acquiring communications data. Prior to the completion of the relevant paperwork it may be advisable to consult with the SPoC.

The Designated Person

The Designated Person (DP) is a person holding a prescribed office in a relevant public authority and who considers the application for Authorisation much the same as a Surveillance RIPA application.

Individuals who undertake the role of a designated person must have current working knowledge of human rights principles, specifically those of necessity and proportionality, and how they apply to the acquisition of communications data.

The Designated person must hold a position within the Council that meets the level specified in the Act and in particular noted in *SI 2010 No.480 Investigatory Powers, The Regulation of Investigation Powers (Communications Data) Order 2010.*

The designated person shall assess the necessity for any conduct to acquire or obtain communications data taking account of any advice provided by the SPoC. They will also assess the issue of proportionality taking into account any meaningful collateral intrusion issues. These responsibilities take place prior to seeking approval by a JP.

Designated persons should not be responsible for granting Authorisations or giving Notices in relation to investigations or operations in which they are directly involved,

The Single Point of Contact

The single point of contact (SPoC) is either an accredited individual (Home Office Course) or a group of accredited individuals trained to facilitate lawful acquisition of communications data and effective co-operation between a public authority and CSPs. They will have been issued a SPoC Personal Identification Number (PIN). Details of all accredited individuals are available to CSP's for authentication purposes.

Under no circumstances will a SPoC allow anyone to use their PIN number.

An accredited SPoC promotes efficiency and good practice in ensuring only practical and lawful requirements for communications data are undertaken. The SPoC provides objective judgement and advice to both the applicant and the designated person. In this way the SPoC provides a "guardian and gatekeeper" function ensuring that public authorities act in an informed and lawful manner.

SPoC's should be conversant with their role and all the relevant contents within the codes of practice.

The SPoC should be in a position to:

- engage proactively with applicants to develop strategies to obtain communications data and use it effectively in support of operations or investigations;

- assess whether the acquisition of specific communications data from a CSP is reasonably practical or whether the specific data required is inextricably linked to other data

- advise applicants on the most appropriate methodology for acquisition of data where the data sought engages a number of CSPs;

- advise applicants and designated persons on the interpretation of the Act, particularly whether an Authorisation or Notice is appropriate;

- provide assurance to designated persons that Authorisations and Notices are lawful under the Act and free from errors;

- provide assurance to CSPs that Authorisations and Notices are authentic and lawful;

- assess whether communications data disclosed by a CSP in response to a Notice fulfils the requirement of the Notice;

- assess whether communications data obtained by means of an Authorisation fulfils the requirement of the Authorisation;

- assess any cost and resource implications to both the public authority and the CSP of data requirements.

The SPoC will retain the original of all the documents involved in the process. Copies of the documents may be retained by the applicant, Designated Person or within the relevant department for audit and filing purposes.

For the purposes of Huntingdonshire District Council, to demonstrate fairness, all three roles will be performed within the application process by separate officers.

The Senior Responsible Officer

The senior responsible office will be responsible for:

- the integrity of the process in place within the public authority to acquire communications data;

- compliance with Chapter II of Part I of the Act and with this code;

- oversight of the reporting of errors to Interception of Communications Commissioners Office (IOCCO) and the identification of both the cause(s) of errors and the implementation of processes to minimise repetition of errors;

- engagement with the IOCCO inspectors when they conduct their inspections, and

- where necessary, oversee the implementation of post-inspection action plans approved by the Commissioner.

The SRO will liaise with the Council's SPoC's and DP's to ensure that the relevant systems and knowledge are of a required standard to comply with their role.

The Application Process

On 1 November 2012 a significant change came into force that effects how local authorities use RIPA to access Communications Data. There is now a requirement under the amendments in the Protection of Freedoms Act 2012, following the acquisition of the Communications Data being authorised by the DP to seek the approval of Local Authority Authorisations and Notices under RIPA by a Justice of the Peace (JP). A Judicial Application/Order form will be completed by either the SPoC or the applicant will be required to attend court and seek the approval of the Justice of the Peace. The original application and a copy will have to be produced to the JP who will either approve or refuse it. The original application will then be retained together with a copy of the Judicial Application/Authorisation form. A copy of the original application form will be retained by the JP.

Prior to an applicant applying for communications data the applicant should contact a SPoC who will be in a position to advise them regarding the obtaining and use of communications data within their investigation. This will reduce the risk of the applicant applying for data which we are not able to obtain and it will also assist the applicant to determine their objectives and apply for the most suitable data for those particular circumstances.

Necessity and Proportionality

The acquisition of communications data under the Act will be a justifiable interference with an individual's human rights under Article 8 of the European Convention on Human Rights only if the conduct being authorised or required to take place is both necessary and proportionate and in accordance with law. Designated Persons who can authorise applications on behalf of this Council will need to have some training with regard to the Human Rights Act and in particular necessity, proportionality and the collateral intrusion issues which may arise with regard to obtaining Communications Data.

The designated person must believe that the conduct required by any Authorisation or Notice is necessary. They must also believe that the conduct to be proportionate to what is sought to be achieved by obtaining the specified communication data – that the conduct is no more than is required in the circumstances. This involves balancing the extent of the intrusiveness of the interference with an individual's right of respect for their private life against a specific benefit to the investigation or operation being undertaken.

Consideration must also be given to any actual or potential infringement of the privacy of individuals who are not the subject of the investigation or operation. They should consider any meaningful degree of collateral intrusion.

Designated Persons should give particular consideration to any periods of days or shorter periods of time for which they may approve for the acquisition of data. They should specify the shortest period in which the objective for which the data is sought can be achieved. To do otherwise will impact on the proportionality of the Authorisation or Notice and impose unnecessary burden upon a CSP given such Notice.

What Forms Will be Used

Below is a list of forms which will be used for the process of obtaining Communications Data. The SPoC's complete most of the forms once the application has been submitted. The SPoC's will therefore ensure that they have the necessary knowledge in how to complete the required paperwork.

- Application Form (to be completed by applicant)
- SPoC Officers Rejection Form (to be completed by the SPoC if necessary)
- SPoC Officers Log Sheet (to be completed by the SPoC)
- SPoC Officers section of the application form
- Draft Notice (to be completed by the SPoC)
- Authorisation form (to be completed by the SPoC if necessary)
- Schedule form (to be completed by the applicant for consequential data)

- Applicants Cancellation Form (to be completed by applicant when necessary and forwarded to the SPoC)

- Notice Cancellation Form (to be completed by the SPoC and forwarded to relevant CSP)

- Authorisation Cancellation Form (to be completed by the SPoC when necessary)

- Error Reporting Letter (to be completed by the SPoC and forwarded to Interception of Communications Commissioners Office (IOCCO)

Up to date version of some these forms can be obtained from the Home office Website http://www.homeoffice.gov.uk/publications/counter-terrorism/ripa-forms other forms can be obtained from the intranet page at HDC.

Application

All applications will be submitted by the applicant in writing using the application forms which can be obtained from the Home Office website to ensure they are relevant and up to date. All the relevant sections should be completed fully as the DP can only consider authorization based on the content of the application form. The details contained within the application form must take account of the objectives, necessity, proportionality and any meaningful degree of collateral intrusion. Should it be determined from advice from the SPoC that consequential data such as telephone subscriber information is likely to be required when applying for an itemized bill; this should be explained on the application form. The SPoC will provide advice regarding these issues and completion of the form.

Schedule

The purpose of this form is to obtain consequential data (additional data) from the data obtained in the initial application form. For example, an application form is submitted for itemised billing on a particular number with a view to analysing the data within it, and then apply for relevant subscriber checks from that itemised bill. The additional subscriber checks will be regarded as consequential data. However, the fact that the applicant is likely to require the data needs to be explained within the initial application form and authorised by the DP.

The applicant would decide which subscriber checks were required and detail them within the schedule form, which will then be submitted to the SPoC. As the data is subscriber information, it would be possible for the SPoC to obtain this data in circumstances where the CSP will agree to provide the data by way of an authorisation, without the need for fresh applications and Judicial Approval. However, if the CSP requires a notice to be served on them prior to providing the data, there will be a requirement to complete an additional application form and seek approval from a JP, following the normal application process. The time limit of one month applies as mentioned earlier. The SPoC will advise the applicant regarding this process.

Within a schedule form, there is the requirement for the applicant to carry out open source enquiries prior to applying for the consequential data. Many telephone numbers and the businesses or persons connected to the numbers, are detailed on the internet. This information can subsequently eliminate the telephone number from the enquiry, or provide valuable intelligence material for the investigator. The test of necessity and proportionality are required when applying for consequential data. It is unlikely to be necessary to obtain a subscriber check on a telephone number, which if checked via the internet would have revealed that it was a bank or something similar. Applicants are required to sign the schedule form to say that they have carried out these types of enquiries. The inspectors, upon carrying out an inspection are likely to check whether the open source enquiries have been carried out. Under no circumstances should data be applied for using the schedule without the open source enquiries being completed. A record of the enquiries undertaken should be maintained. This is also a requirement under the Criminal Procedures Investigations Act (CPIA).

Renewal of Authorisations and Notices

Renewals would normally be used when obtaining future data such a cell site analysis which this Council is not allowed to obtain. However, in the rare event the SPoC believes it necessary and appropriate to renew an application for whatever reason, they will advise the applicant on the appropriate process to be followed and Judicial Approval will be required.

The original application, Notice/ Authorisation (or copy if original has been served on CSP) will be retained by the SPoC within a central records held by the Fraud Team.

Cancellation of Notices and Withdrawal of Authorisations

A cancellation will be appropriate when an Authorisation or Notice has been authorised and prior to receiving or obtaining the Data from the C.S.P. it becomes apparent that the data requested is no longer required, or no longer proportionate to what was sought to be achieved.

In these situations it is the responsibility of the applicant or other officers conducting the investigation to ensure that they notify the SPoC as soon as it becomes apparent that the data is no longer required. The notification to the SPOC should be done in such a way as to produce a written record such as by email. An Application Cancellation form, which can be obtained from the Home Office Website or HDC intranet/SPOC, should be submitted by the applicant and a cancellation of the Authorisation or Notice form should be signed by the originating DP (or another DP in their absence) which will then be served on the CSP by the SPoC

It will be at the discretion of the SPoC to decide whether they feel it necessary to inform the CSP prior to serving a cancellation Notice.

Urgent Oral Authorisation

There is no provision within the legislation for the Council to orally provide authority to obtain Communications Data. All requests will be made in writing on the appropriate application forms.

Costs

There may be costs incurred when obtaining Communications Data from CSP's. It will be the responsibility of the SPoC to assess the costs involved and advise the DP prior to Authorisation. The SPoC will also provide advice to applicants to ensure that no unnecessary costs are incurred.

Records

Security of Records and Data

All the records and any data obtained as a result of the process under this legislation must be kept secure and confidential.

Applications, Authorisations, Judicial application/approval forms, copies of Notices, and records of the withdrawal of Authorisations and the cancellation of Notices, must be retained by the Council in written or electronic form, and physically attached or cross-referenced where they are associated with each other. The Council will also keep a record of the date and, when appropriate to do so, the time when each Notice or Authorisation is given or granted or cancelled. Errors should they occur (see below) will also be recorded by the SPoC and notified to the Senior Responsible Officer. These records will be held centrally by the SPoC.

These records must be available for inspection by the Commissioner and retained to allow the Investigatory Powers Tribunal to carry out its functions

Record of Activity

To meet its requirements the Council must also keep a record of the following items:

- number of applications submitted to a designated person for a decision to obtain communications data which were rejected after due consideration;

- number of Notices requiring disclosure of communications data within the meaning of each subsection of section 21(4) of the Act or any combinations of data;

- number of Authorisations for conduct to acquire communications data within the meaning of each subsection of section 21(4) of the Act or any combinations of data;

This record will be maintained by the SPoC and must be sent in written or electronic form to the Commissioner when requested by him.

Errors

The thorough checking of applications and this Council's operating procedures, including the careful preparation and checking of applications, Notices/Authorisations, should reduce the scope for making errors. Attention to detail will be required by all persons involved in the process.

Reporting and recording of errors will draw attention to those aspects of the process of acquisition and disclosure of communications data that require further improvement to eliminate errors and the risk of undue interference with any individual's rights. Therefore the SPoC will bring to the immediate attention of the SRO of either a recordable error or a reportable error and the necessary action can then be taken in line with the Codes of Practice.

Where material is disclosed by a CSP in error which has no connection or relevance to any investigation or operation undertaken by the public authority receiving it, that material and any copy of it should be destroyed as soon as the report to the Commissioner has been made.

An error can only occur after a designated person:

- has granted an Authorisation and the acquisition of data has been initiated, or
- has given Notice and the Notice has been served on a CSP in writing, electronically or orally.

It is important to apply the procedures correctly to reduce the risk of an error occurring.

Where any error occurs, a record should be kept.

There are two types of errors:

- Reportable
- Recordable

Reportable

Where communications data is acquired or disclosed wrongly a report must be made to the Commissioner **("reportable error")**. Such errors can have very significant consequences on an affected individual's rights with details of their private communications being disclosed to a public

authority and, in extreme circumstances, being wrongly detained or wrongly accused of a crime as a result of that error. (see below for some examples of reportable errors).

Recordable

In cases where an error has occurred but is identified by the public authority or the CSP without data being acquired or disclosed wrongly, a record will be maintained by the public authority of such occurrences **("recordable error").** These records must be available for inspection by the Commissioner. (see below for some examples of recordable errors).

The staff involved in the process of acquiring Communications Data must adhere and report errors once they have been identified. It will not be acceptable for the error to be ignored. It will be the responsibility of SPoC's and the Senior Responsible Officer to be aware of the different ways in which errors can occur and the relevant procedure to be followed. Some examples are detailed below. They will also be responsible for informing applicants to report any errors that they are aware of to the SPoC.

Examples can include:

Reportable Errors

- an Authorisation or Notice made for a purpose, or for a type of data, which the relevant public authority cannot call upon, or seek, under the Act;

- 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 a public authority when engaging in conduct specified in an Authorisation;

Recordable errors

- a Notice given which is impossible for a CSP to comply with and an attempt to impose the requirement has been undertaken by the public authority;

- failure to review information already held, for example unnecessarily seeking the acquisition or disclosure of data already acquired or obtained for the same investigation or operation, or data for which the requirement to acquire or obtain it is known to be no longer valid;

Excess Data

Where an application by this Authority results in the acquisition of excess data, or its disclosure by a CSP in order to comply with the requirement of a Notice, all the data acquired or disclosed will be retained by the public authority.

As the material will have been obtained in connection with a criminal investigation it is bound by the Criminal Procedures Investigations Act (CPIA) and its code of practice and therefore there will be a requirement to record and retain data which is relevant to the criminal investigation, even if that data was disclosed or acquired beyond the scope of a valid Notice or Authorisation. If the criminal investigation results in proceedings being instituted all material that may be relevant must be retained at least until the accused is acquitted or convicted or the prosecutor decides not to proceed.

If having reviewed the excess data it is intended to make use of the excess data in the course of the investigation or operation, the applicant must set out the reason(s) for needing to use that material in a report which will be an addendum to the application upon which the Authorisation or Notice was originally granted or given. This will be submitted via the SPoC who will forward the relevant documentation to the Designated Person who will then consider the reason(s) and review all the data and consider whether it is necessary and proportionate for the excess data to be used in the investigation or operation.

Criminal Procedures and Investigations Act (CPIA) and the Data Protection Act (DPA)

The codes do not affect any other statutory obligations placed the Council to keep records under any other enactment such as the Criminal Procedure and Investigations Act 1996 (CPIA) This requires that material which is obtained in the course of an investigation and which may be relevant to the investigation must be recorded, retained and revealed to the prosecutor.

Data Protection Safeguards

Communications data acquired or obtained under the provisions of the Act, 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 must be adhered to.

There is no provision in the Act preventing CSPs from informing individuals about whom they have been required by Notice to disclose communications data in response to a Subject Access Request made under section 7 of the DPA. However, a CSP may exercise certain exemptions to the right of subject access under Part IV of the DPA.

Section 29 provides that personal data processed for the purposes of the prevention and detection of crime; the apprehension or prosecution of offenders, or the assessment or collection of any tax or duty or other imposition of a similar nature are exempt from section 7 to the extent to which the application of the provisions for rights of data subjects would be likely to prejudice any of those matters. However this is not an automatic right. In the event that a CSP receives a subject access request where the fact of a disclosure under the Act might itself be disclosed the CSP concerned must carefully consider whether in the particular case disclosure of the fact of the Notice would be likely to prejudice the prevention or detection of crime.

Should a request for advice be made from a CSP regarding a disclosure the SPoC will consult with the Data Protection Officer of the Council and Head of Legal Services if necessary before a decision is made. Each case should be examined on its own merits.

Equally these rules will apply should a subject access request be made from an individual where material under this legislation is held by the Council.

A record will be made of the steps taken in determining whether disclosure of the material would prejudice the apprehension or detection of offenders. This might be useful in the event of the data controller having to respond to enquiries made subsequently by the Information Commissioner, the courts and, in the event of prejudice, the police.

Should the Council have a request to obtain or disclose Communications Data to an overseas authority this request will be notified to the SPoC. All parties involved should refer to the section covering this area within the Codes of Practice and they should also take advice from the Council's Data Protection Officer.

It will be the responsibility of the SPoC to ensure that they are aware of how acquiring Communications Data impacts on the Data Protection Act.

Training

The Senior Responsible Officer will have responsibility for ensuring appropriate training for staff mentioned within this policy and for retaining a record of that training.

Reporting to Members

Annual returns of all activity undertaken by Council staff will be compiled by the Senior Responsible Officer and provided to the Corporate Governance Panel annually in line with the current advice in the Codes of Practice. Members will review on a yearly basis the policy to assess whether the activity undertaken is in line with this policy.

Oversight

The Act provides for an Interception of Communications Commissioner ('the Commissioner') whose remit is to provide independent oversight.

It is important to note that should the Commissioner establish that an individual has been adversely affected by any willful or reckless failure by any person within a relevant public authority exercising or complying with the powers and duties under the Act in relation to the acquisition or disclosure of communications data, he shall, subject to safeguarding national security, inform the affected individual of the existence of the Tribunal and its role. The Commissioner should disclose sufficient information to the affected individual to enable him or her to effectively engage the Tribunal.

Complaints

The Act established an independent Tribunal

Details of the relevant complaints procedure can be obtained from the following address:

The Investigatory Powers Tribunal
PO Box 33220
London
SW 1H 9ZQ
020 7035 3711

ADVICE

If you require further advice about covert surveillance, please contact the Fraud Team (SPoC Officers) based at Pathfinder House.

POLICY UPDATING PROCEDURE

Proposed amendments to this Policy must be forwarded to the Senior Responsible Officer where they will be considered in consultation with Fraud Team (SPoC Officers) before submission to Chief Officers Management Team and Cabinet.

The Policy shall be reviewed as required by legislation, upon advice from the Home Office or following an inspection by the IOCCO.

FURTHER INFORMATION ENQUIRIES AND COMPLAINTS

The Senior Responsible Officer is the first point of contact on any of the matters raised in this policy statement. Enquiries should be addressed to :

The Head of Legal & Democratic Services
Pathfinder House
Huntingdonshire District Council
Pathfinder House
St Mary's Street
Huntingdon
Cambridgeshire
PE29 3TN
Tel : (01480) 388388

Nick Jennings
Fraud Manager
1.5.2013

ANNEX A

LIST OF OFFICERS ROLES

ROLE	SERVICE	POST	POST HOLDER
Senior Responsible Officer	Council-Wide	Head of Legal and Democratic Services	Colin Meadowcroft
(Senior) Designated Person	Council-Wide	Head of Paid Service	Malcolm Sharp
Designated Person	Customer Services	Head of Customer Service	Julia Barber
Designated Person	Environmental Health and Community Services	Head of Environmental Health Services	Sue Lammin
Designated Person	Planning Services	Head of Planning Services	Steve Ingram
Designated Person	Head of Operations Division	Head of Service-Operations Division	Eric Kendall
SPoC Officers	Fraud Team		Nick Jennings Loraine Southworth Cindy Dickson