POLICY & GUIDANCE NOTES
ON
ACCESSING COMMUNICATIONS DATA
Under the
REGULATION OF INVESTIGATORY POWERS ACT 2000.

Communications Data

This section gives guidance on the requirements of RIPA when obtaining communications data from a Communication Service Provider (CSP) and must be read in conjunction with the **Accessing Communications Data Draft Code of Practice** (http://www.homeoffice.gov.uk/docs/pcdcpc.html).

Communications data includes information relating to the use of a postal service or telecommunication system but **does not** include the contents of the communication itself, contents of e-mails or interactions with websites.

Any person engaged in the obtaining of such information must be properly authorised and act with that authority. Each Directorate shall have a Designated Officer who is not lower in rank than Chief Officer or is 'the officer responsible for the management of the investigation', this may be the Head of Service with responsible for that investigation/enforcement activity . This is to ensure that the person giving the authorisation, whilst understanding the work being done, is sufficiently divorced from the actual activity to make an objective judgement.

Local Authorities may only obtain communications data for the purpose of preventing or detecting crime or of preventing disorder.

The Designated Officer must consider both necessity and proportionality before communications data is obtained. Access to communications data may be authorised in two ways:

1. Through an authorisation order in which case the Council will collect or retrieve the data itself.

Or

2. By a notice in which case a notice is given to the Communication Service Provider (CSP) to collect or retrieve the data and provide it to the Council.

A Designated Officer decides whether or not an authorisation should be granted or a notice given. The authorisation only authorises the conduct of obtaining communications data. Both the application form and the authorisation are not served on the CSP but are retained by the department. The authorisation should be in a standard written format and information recorded must include a unique reference number.

Notices are served on the CSP but will only contain enough information allow them to fulfil their duties under RIPA. The notice should also contain the unique reference number.

Oral authorisations may only be made in exceptional circumstances 'for the purpose, in an emergency, of preventing death or injury or any damage to a person's physical or mental health, or of mitigating any injury or damage to a person's physical or mental health'.

Both the applicant and Designated Officer must record oral authorisations at the time or as soon as possible. Authorisations and notices are valid for one month and this period begins when the authorisation is granted or notice given.

The Designated Officer must cancel all authorisations and notices as soon as they are no longer necessary or the conduct no longer proportionate to what is sought to be achieved. In the case of notices, the relevant CSP operator should be informed of the cancellation. Applications, authorisations and notices for communications data must be retained until the Communications Commissioner has audited them.

Each Local Authority must have at least one person who is the Single Point of Contact (SPOC) whom all notices and authorisations should be channelled through and who will be the only person that deals with the CSPs. The reason for this is that there must be a specific point of accountability in each authority requesting data, not least for oversight purposes, but also should the legality of the request be contested e.g. on human rights grounds. Therefore there cannot be a regional SPOC, or any SPOC, which covers more than one authority although it is allowed to have more than one SPOC within a Local Authority.

A SPOC will also provide for an efficient regime and assist in reducing the burden on the CSP by such requests. The SPOC will amongst other things, be able to advise Designated Officers on whether an authorisation or notice is appropriate, the validity of the application and the practicality of obtaining the data.

SPOC Training and Assessment Requirements

A Local Authority officer can only become a Home Office accredited SPOC after attending appropriate training and undergoing subsequent assessment. Subject to assessment, the Home Office will then issue the SPOC with a PIN number which will be recognised by all CSPs and enable them to access communications data under RIPA.

This PIN number is unique to each SPOC. It is not for the entire Local Authority to use and pass around to different investigators or different investigation departments. It is be beneficial for Designated Person(s) to also attend SPOC training although this is not a requirement at present.

The SPOC for HDC will be located within the Fraud Investigation Team of the Revenue Services Department. A number of officers within that Team will retain Home Office accreditation to ensure that a comprehensive service is provided across the authority.

All forms, pro-formas and documentation used for all such activity will be in format approved and provided by the Home Office for the purpose specified. Only the latest such documentation will be used by downloading from the Home Office website.

Appendix 2: List of Designated Officers

DIRECTORATE /SERVICE	NAME	COMMENTS
Council-wide	Chief Executive	
Administration Management	Head of Administration	
Legal and Estates	Head of Legal and Estates	
Directorate of Commerce & Technology	Director	
Revenue Services	Head of Revenue Services	
Financial Services	Head of Financial Services	
Internal Audit	Audit Manager	
Information Management Department	Head Information Management Department & Customer First	
Community Services	Head of Community Services	
Directorate of Operational Services	Director	
Planning Services	Head of Planning Services	
Environmental Health Services	Head of Environmental Health Services	
Environment and Transport	Head of Environment and Transport	
Housing Services	Head of Housing Services	
Operations Management	Head of Operations	

Nick Jennings Benefits Fraud Manager