DERBY CITY COUNCIL

COUNCIL CABINET
4 SEPTEMBER 2007

ITEM 11

Cabinet Member for Corporate Policy

Inspection by the Interception of Communications Commissioner's Office (IOCCO)

SUMMARY

1.1 On 5 March 2007 an Inspector from the IOCCO's office visited the Council to carry out an inspection of the Council's arrangements for the acquisition of "Communications Data" under the Regulation of Investigatory Powers Act 2000 (RIPA).

1.2 The primary purpose of the Inspector's inspection was to ensure that:

- the Council's systems for acquiring communications data are sufficient for the purposes of RIPA;
- relevant records have been kept;
- all accessing of communication data has been carried out lawfully and in accordance with the Human Rights Act and RIPA;
- the data which has been obtained is necessary and proportional;
- officers engaged in the acquisition of data are adequately trained and aware of the relevant legislation.

1.3 The Inspector submitted a report on his inspection to the Council on 5 June 2007 and this has 10 Action Points, which are set out in Appendix 2 of this report. This report is a response to those Action Points.

RECOMMENDATIONS

2.1 To accept the Action Points in the IOCCO's Inspector's report at Appendix 2.

2.2 To approve and adopt the draft policy document on RIPA Communications Data attached at Appendix 3

2.3 To approve the following appointments for the purposes of the Council's RIPA Communications policy:

- "Single Point of Contact" (SPoC) – Melvyn Smith, Trading Standards Manager, with Mark Holmes, Benefits Manager acting as reserve;
- Authorised Officer – Assistant Director, Environmental Health and Trading Standards, with the Principal Solicitor (Litigation), Legal Division acting as a reserve;
- Senior Responsible Officer – Chief Legal Officer.

REASON FOR RECOMMENDATIONS

3.1 To meet the requirements of the IOCCO report.

DERBY CITY COUNCIL

COUNCIL CABINET
4 SEPTEMBER 2007

ITEM

Report of the Corporate Director for Corporate and Adult Services

Inspection by the Interception of Communications Commissioner's Office (IOCCO)

SUPPORTING INFORMATION

1.1 Part I of the Regulation of Investigatory Powers Act 2000 (RIPA) enables the Council, as a designated public body, to acquire in the course of criminal investigations, such as Trading Standards and Housing Benefit cases, certain communications data.

1.2 "Communications data" for this purpose is information held by "Communication Service Providers" ("CSP"), such as telecom, internet and postal companies, about communications made by their customers. It includes information about the use of a postal service or telecommunications system but **not** the content of the communication itself. For example, data available to the Council under the Act includes:

- Postal items - anything written on the outside of the envelope
- Telephone subscriber information – personal details of the subscriber, the phone number and itemised calls made;
- Email and internet subscriber information – details of the subscriber of the email account, websites visited, details of the date and time of emails sent and received (but **not** the content of them).

1.3 The Interception of Communications Commissioner's Office (IOCCO) has oversight responsibilities for ensuring that public bodies that have access to and utilise these statutory powers do so in a manner that is transparent, fair and is in keeping with the principles of the Human Rights Act.

1.4 As part of the process of undertaking its oversight responsibilities, the IOCCO carries out inspections of the facilities and processes in place within such public bodies. The Council was inspected as part of that process on 5 March 2007 by one of the Commissioner's inspectors.

1.5 The inspector reported back to the Council on 5 June 2007. Within the report was an action plan incorporating his recommendations to the Council aimed at ensuring that the processes we have in place comply with the RIPA and the relevant code of guidance. The action plan is set out in Appendix 2.

1.6 Officers have met and have considered the Inspectors' Action Plan and at Appendix 3 is the text of a draft policy on communications data, which addresses all the points in the Plan. The final column in Appendix 2 cross-references the Action Plan recommendations to the relevant paragraph in the draft Council policy.

1.7 If approved, the policy will be incorporated into the existing corporate policy document that deals with directed surveillance and the use of covert human intelligence sources to create one composite RIPA guidance document.

1.8 Compliance with the legislative requirements also entails a number of formal appointments being made to give effect to the inspector's recommendations. Three posts are advocated namely, Single Point of Contact (SPoC), Authorised Officer and Senior Responsible Officer.

1.9 SPoCs are required to be trained and individually accredited to enable them to exercise the powers of their office. Inevitably, this means that appointments to the post must be by reference to name, rather than professional designation. They act as the conduit for the transmission of applications between the Council and the CPS's.

1.10 The SPoCs are also expected to promote good practice and provide informed advice to both the Applicant and the Authorising Officer to ensure only practical and lawful data requests are made. In addition it is envisaged that the SPoC will be responsible for maintaining the central register of authorisations issued by the Council.

1.11 Authorised Officers are responsible for quality assuring the detail contained in applications, with the express aim of satisfying themselves that the tests of necessity, proportionality and limited collateral intrusion are met.

1.12 The Senior Responsible Officer's role is primarily to assist the Commissioner in his oversight responsibilities by ensuring compliance with the communications data provisions of the 2000 Act.

1.13 It is therefore proposed that each of the posts referred to are occupied as follows:

- SPoC – Melvyn Smith, Trading Standards Manager, with Mark Holmes, Benefits Manager acting as reserve in his absence ;

- Authorised Officer – Assistant Director, Environmental Health & Trading Standards, with the Principal Solicitor (Litigation), Legal Division acting as reserve in his absence;

- Senior Responsible Officer – Chief Legal Officer.

OTHER OPTIONS CONSIDERED

2. No other options were considered as it is thought necessary for the Council to act in accordance with the letter and spirit of the RIPA legislation.

For more information contact:	Olu Idowu olu.idowu@derby.gov.uk Tel: 01332 255675
Background papers:	
List of appendices:	Appendix 1 – Implications Appendix 2 – Action Points from IOCCO Inspector's Report Appendix 3 – Draft Policy documentation on RIPA Communications Data

IMPLICATIONS

Financial

1. Any training requirements will be met from existing budgets.

Legal

2. As set out in the report.

Personnel

3. None.

Equalities impact

4. None.

Corporate priorities

5. Investigations under RIPA help **Reduce crime**

Appendix 2

No.	Action Points	Agreed	Progress	Comments
	Applicant Level			
1.	Para 4.1 – It would be good practice to personalise the new application form to Derby City Council and make it available to all potential applicants on the Council's intranet site to ensure the application form is standardised.			Done – Forms in Document Library all include the Council name and corporate logo [see paragraph 1.12 of draft policy]
2.	Para 4.2 – It is recommended that all purposes other than Section 22(2)(b) are removed from the application form.			Done – Forms in Document Library all amended to show the single statutory purpose of 'prevention and detection and crime' in line with paragraph 1.3 of draft policy
3.	Para 4.10 – Recommend that applicants are provided with advice in relation to the principles of necessity, proportionality and collateral intrusion, as outlined in Paragraphs 4.6 to 4.8 of this report, to improve the quality of the applications and focus applicants to ensure they provide the key information.			Done – see paragraphs 1.4 to 1.6 of draft policy
	SPoC			
4.	Para 4.15 – It is recommended that the AO should maintain a SpoC log sheet for each application in accordance with the advice given in Paragraphs 4.14 to 4.15 of the report to ensure there is an audit trail of all of the actions taken by the AO from the start to the end			Done – see paragraph 1.14 of draft policy

	of the process.			
5.	Para 4.16 – Recommend that the AO should start to quality assure the applications which are made to assist to improve the quality of the applications submitted and to ensure that any future applications meet the required standard.			Done – see paragraph 1.15 of policy document

No.	Action Points	Agreed	Progress	Comments
	SpoC Continued…			
6.	Para 4.17 – The SpoC within the Trading Standards Team needs to ensure it is achieving a fairly good level of compliance and in the future we would recommend that if another department, such as the Housing and Council Tax Benefits Investigations Team, needs to acquire communications data, that they use the SpoC within the Trading Standards Team.			Not agreed. Letter sent to the IOCCO explaining the Council's reasoning. Reply since received confirming the IOCCO does not take issue with the Council's approach.
	Designated Persons Approvals			
7.	Para 4.23 – Recommend that the DP should tailor their written considerations to the individual application, following the advice given in Paragraphs 4.21 to 4.23 of this report, as this is the best means of demonstrating that it has been properly considered.			Done – see paragraph 1.16 of draft policy
	Content of Authorisations and Notices			
8.	Paragraph 4.26 – Recommend the Council uses the new S22(4) Notice template as it contains purely the information necessary for compliance with the Act and draft CoP and as such should streamline the process further.			Done – Forms in Document Library all revised to replicate the template provided
	Senior Responsible Officer			
9.	Para 4.29 – It is recommended that the Council should appoint an SRO and develop a policy and operating guidelines in relation to the acquisition and disclosure			Done – See paragraph 1.10(iv) of draft policy

	of communications data.			
	Record Keeping			
10.	Para 5.2 – Recommended that the application form, SpoC log sheet and Notice should all be marked 'Restricted' in accordance with the Government Protected Marking Scheme.			Done – Forms in Document Library all revised to incorporated the term 'Restricted'

Appendix 3

1. COMMUNICATIONS DATA

1.1 Communications data is information held by Communication Service Providers (CSP) (e.g. telecom, internet and postal companies) relating to the communications made by their customers. The 2000 Act makes provision for obtaining communications data from such service providers and the disclosure to any person of such data. For these purposes, 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 (i.e. traffic data - contents of e-mails).

1.2 Examples of "data" available to the Council under the Act include:

- Postal items - anything written on the outside of the envelope
- Telephone subscriber information - personal details of the subscriber, the telephone number and itemised calls made.
- E-mail & Internet subscriber information – details of the subscriber of email account, websites visited, details of the date and time emails sent and received.

1.3 Similarly to the procedures relating to both directed surveillance and CHIS, communications data can only be obtained for the sole category of **for the prevention and detection of crime and/or disorder**. There is also the requirement to ensure that the test of **necessity** is met before data is obtained. It is the responsibility of the Authorising Officer to undertake that test. In addition, the Authorising Officer must also consider that the conduct involved in obtaining the communications data is **proportionate** to the aim that it is sought to achieve. In carrying out these assessments, the Authorising Officer must remain alert to the risk of collateral intrusion which is to be avoided unless such intrusion can be justified.

1.4 The principle of **necessity** requires that applicant's must ensure that they specify the particulars of the offence under investigation, ideally by reference to the applicable legislative provision that has been breached. A short explanation of the offence, the details of the perpetrator, the victim or witness and the telephone or internet address, and how each of these link in with the application being made should be detailed. The source of the telephone number or internet address should also be outlined.

1.5 The principle of **proportionality** requires an explanation from the applicant about why specific date or time periods of data are being sought, and what the applicant expects to achieve from obtaining the data. Doing so should enable applicants to demonstrate how the level of intrusion is considered to be justified when taking account of the benefit to be derived from acquiring the data. It may be prudent at this stage to outline what other less intrusive forms of investigation have been considered or tried, and why the applicant deems such measures either to not be feasible or to have failed.

1.6 The principle of **collateral intrusion** requires the applicant to demonstrate that s/he has considered the likelihood that through the process of acquiring the data, they are aware of the possibility that they might obtain information that is outside the realms of the investigations in question and then outline how, if that occurs, they plan to manage that process and/or the information so obtained.

Applying for Communications Data

1.7 There are two independent routes by which the Act allows communications data to be obtained from service providers. These are either: -

(i) the granting of **Authorisations;** or
(ii) the service of **Notices**

Authorisation

1.8 An Authorisation allows the Council to collect or retrieve data itself from the CSP. An authorisation may be appropriate where:

- the postal or telecommunications operator is not capable of collecting or retrieving the Communications Data;
- it is believed that the investigation may be prejudiced if the postal or telecommunications operator is asked to collect the data itself;
- there is a prior agreement in place between the Council and the postal or telecommunications operator as to the appropriate mechanisms for the disclosure of communications data.

Notice

1.9 This is the more likely method by which communications data will be retrieved by the Council. A Notice is given by the Council to a postal or telecommunications operator that requires the operator to collect the data and provide it to the Council.

Roles

1.10 Within the Council, there are four distinct roles involved in the process of accessing/obtaining communications data, namely:

(i) The **applicant** is the person involved in conducting an investigation or operation. Within the Council, this would normally be the case officer. The applicant begins the process by completing an application form, setting out within the form for consideration by the Authorising Officer sufficient detail justifying the need for the data in question to be accessed;

(ii) The applicant then forwards the application to the Council's **Single Point of Contact (SPoC)**. The SPoC is an accredited individual (and hence is sometimes referred to as an Accredited Officer) trained in the process of facilitating the lawful acquisition of communications data and acts as the go-between between the Council and the CSP;

(iii) The SPoC will forward the application to the **Authorising Officer**. It is the role of the Authorising Officer to satisfy him or her self about the necessity and proportionality of the application, and that there either is no collateral intrusion involved in the investigation

or that any such intrusion is justifiable. They will make that assessment strictly on the basis of the information contained in the application. If so satisfied, they sign off the application and return it to the SPoC, who then sends it to the CSP;

(iv) The **Senior Responsible Officer** is responsible for ensuring the integrity of the process in place within the Council for acquiring communications data. The post holder is responsible for ensuring compliance with the communications data provisions of the 2000 Act, the oversight responsibility for identifying errors, ensuring that adequate processes are in place to minimise repetition of errors and reporting of errors to the Commissioner.

1.11 Details of the posts within the Council that undertake each of these roles are contained in Appendix 4. In relation to the Authorising Officer role, it is anticipated that the vast majority of authorisations will be granted/issued by the Assistant Director – Environmental Health & Trading Standards, with the Principal Solicitor (Litigation) occupying his post as a reserve. Likewise in relation to the SPoC office, it is again anticipated that the majority of applications will be processed by the Trading Standards Manager, with the Benefits Manager occupying his post as a reserve.

The Application Process

1.12 An application for accessing communications data needs to be completed together with the Notice. As with the other methods of surveillance, these forms have been standardised by the Council and are available within the document library on DerbyNet. The applicant will need the following information to complete these forms:

- a unique reference number (URN)
- the operation and person (if known) to which the requested data relates;
- a description, in as much detail as possible, of the Communications Data requested;
- the reason why obtaining the requested data is considered to be necessary;
- an explanation of why obtaining the data constitutes conduct proportionate to what it seeks to achieve;
- a consideration of collateral intrusion, the extent to which the privacy of others may be affected and why that intrusion is justified;

- the time-scale within which the Communications Data is required. Where the time-scale within which the material is required is any greater than routine, the reasoning for this is to be included.

1.13 An authorised application form should subsequently record whether access to communications data was approved or denied, by whom and the date. Alternatively, the application form can be marked with a cross-reference to the relevant notice. Both the application and the Notice form then need to be checked by the SPoC.

1.14 The SPoC's role, while primarily a conduit for the transmission of information between the Council and the CSP, also promotes good practice by ensuring that only practical and lawful communications data requests are made. The SPoC provides objective judgement and advice to both the applicant and the Authorising Officer. The SPoC will complete a log sheet that records details of each application they have considered, the dates they were received, who from, when forwarded to the Authorising Officer, the date when the Notice (or Authorisation) is returned to the SPoC, when the SPoC forwarded on the Notice to the CSP, when results were received from the CSP and summaries of all communications exchanged between the SPoC and the CSP during the processing of the Notice (or Authorisation).

1.15 The Council has two accredited SPoC's, whose details appear in Appendix 4. It is a requirement that a person carrying out the functions of a SPoC must have successfully completed the relevant SPOC training for the purposes of dealing with communications data. SPoC's should be in a position to:

- assess whether access to communications data is reasonably practical for the postal, internet or telecommunications operator;
- advise applicants and Authorising Officers on the practicalities of accessing different types of communications data from different postal, internet or telecommunications operators;
- advise applicants and Authorising Officers on whether communications data falls under section 21(4)(a), (b) or (c) of the Act;
- provide safeguards for authentication;
- assess any cost and resource implications to both the Council and the postal, internet or telecommunications operator.

Once the SPoC has satisfied himself of these issues, they then forward the application and notice onto the Authorising Officer.

1.16 The Authorising Officer's role is as set out in paragraph 1.3 – to be satisfied that the dual tests of necessity and proportionality are met and that there is no collateral intrusion, or else that any such intrusion can be objectively justified. Where the application is based on grounds of urgency, he or she must also be satisfied that any such grounds are justified. The Authorising Officer will base his or her decision solely on the content of the application form, which is never sent to the CSP. If so satisfied, then they grant an Authorisation or give a Notice. The Authorisation or Notice is then returned to the SPoC for the SPoC to send out to the CSP.

1.17 An Authorising Officer must not grant an Authorisation or give a Notice on a matter in which they are directly involved.

1.18 The Notice served on the CSP must contain the following information:

- a description of the required communications data;
- for which of the purposes the data is required;
- the name, office, rank or position of the Authorising Officer; and
- the manner in which the data should be disclosed.

1.19 The Notice should also contain:

- a Unique Reference Number (URN) obtained from the relevant CSP;
- where appropriate, an indication of any urgency;
- a statement stating that data is sought under the provisions of Chapter II of Part 1 of the 2000 Act i.e. an explanation that compliance with the Notice is a legal requirement; and
- contact details so that the veracity of the Notice may be checked.

1.20 Authorising Officers should be of the same level of seniority as identified within the forms of directed surveillance and CHIS dealt with earlier in this policy document.

Urgent Requests

1.21 An application for communications data may only be made and approved orally, on an urgent basis, where it is necessary to obtain the data in an emergency i.e. where life would be endangered or the investigation jeopardised. Urgent oral authorisations have a duration of 72 hours commencing from the time when the authorisation was granted.

Duration of Authorisations and Notices

1.22 Authorisations and Notices are only valid for **one month**. This period will begin when the Authorisation is granted or the Notice given. The Authorising Officer should specify a shorter period if s/he is satisfied by reference to the detail contained in the request of the appropriateness of doing so, since this may go to the proportionality requirements. For 'future' applications, communications data disclosure may only be required of data obtained by the postal, internet or telecommunications operator **within** a period of up to one month. For 'historical' applications, communications data disclosure may only be required if it is in the possession of the postal, internet or telecommunications operator. A postal, internet or telecommunications operator should comply with a Notice as soon as is reasonably practicable.

Reviews

1.23 Reviews should be undertaken during the authorised period to assess the continuing need for/use of communications data. The frequency of review will be determined by the Authorising Officer in the context of the investigation and taking particular account of access to confidential information and collateral intrusion. Records of review should be forwarded to the SPoC for inclusion in the central record.

Renewal

1.24 An Authorisation or Notice may be renewed at any time during the month it is valid, by following the same procedure as in obtaining a fresh Authorisation or Notice. A renewed Authorisation or Notice takes effect at the point at which the Authorisation or Notice it is renewing expires.

1.25 Authorisation of renewals will normally be made by the original Authorising Officer unless it is not reasonably practicable to do so, in which event the reserve Authorising Officer may authorise renewal. Authorisations may be renewed more than once provided they continue to meet the criteria for Authorisation.

1.26 Application for renewals must include the following information:

- whether this is the first renewal or details of every occasion on which the authorisation has been renewed previously;
- any significant changes to the information supplied in the original application;
- reasons why it is necessary to continue the surveillance;
- content and value to the investigation/operation of the information already obtained;
- result of reviews of the investigation;

Cancellation

1.27 The Authorising Officer should cancel a Notice as soon as 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 primarily falls on the Authorising Officer who issued it.

1.28 In relation to the service of a Notice, the relevant CSP will need to be informed of the cancellation.

1.29 Records of cancellations are recorded on a separate form. An Authorising Officer who cancels a Notice should ensure that they forward notification of the cancellation to the SPoC for recording/retention within the central register.

Guidance

1.30 More detailed guidance for applicants on the principles of necessity, proportionality and collateral intrusion is provided in a separate guidance note 'Guidance to Applicants for Communications Data' which can be found on DerbyNet.

Training

1.31 The Council is committed to ensuring that all of its employees, at whatever level, involved in the administration, processing and acquisition of communications data are properly trained for that purpose. The need for refresher training will be considered at least annually. All employees involved in the communications data process are encouraged to raise any emerging training needs with either of the Council's SPoC's, Authorising Officers or the Senior Responsible Officer.