

## ABERDEEN CITY COUNCIL

<b>Name of Committee</b>	:	Policy & Strategy Committee
<b>Date of Meeting</b>	:	4 March 2008
<b>Title of Report</b>	:	Regulation of Investigatory Powers Act 2000- Corporate Policy and Procedure
<b>Lead Officer</b>	:	Jane MacEachran, City Solicitor, Resources Management
<b>Author of Report</b>	:	Jessica Anderson, Senior Solicitor, Resources Management ☎ (52)2553 ✉ JeAnderson@aberdeencity.gov.uk
<b>Other Involvement</b>	:	None
<b>Consultation undertaken with</b>	:	Trade Unions, Community Planning and Regeneration, Councillors Kate Dean, Neil Fletcher and Kevin Stewart, Corporate Directors for Neighbourhood Services (North, South and Central Areas), Corporate Directors for Resources Management, Continuous Improvement and Strategic Leadership and Trading Standards.

### **Summary of Report**

To seek Committee approval for the attached Corporate Policy related Procedure with respect accessing communications data as covered in the report.

### **Recommendations**

1. To approve the Policy and Procedure attached hereto as a Corporate Policy and Procedure.
2. To permit the City Solicitor to refine the procedure for any further compliance, if necessary, once the external SPoC is in place.

### **Links to the Community Plan and to Vibrant, Dynamic & Forward Looking**

Compliance with the Corporate Policy and Procedure, and with the Council's legal obligations under the Regulation of Investigatory Powers Act 2000 (RIPA) in relation to accessing communications data, will ensure that Council Services do not unlawfully interfere with a citizen's right to privacy whilst that Service is exercising a statutory function.

### **Implementation**

The Policy and Procedure will be published and accessible on the City Solicitor's homepage. Notification of the Policy and Procedure will be delivered via the Council's *Teamtalk* newsletter, the Intranet (The Zone). Officers using the powers under RIPA will be required to be trained prior to using same.

### **Resource Implications**

- People** : Staff must be aware of and be able to correctly implement the Policy and Procedure if required to make an application for access to communications data.
- Finance** : A fee of £50 will required to be paid per application by each Service requesting this type of information.
- Systems & Technology** : Access to the on-line application system will require officers to have internet access.
- Property** : None arising from this report
- Other Equipment** : None arising from this report
- Other** : None arising from this report

### **Other Implications**

- Health & Safety** : None arising from this report
- Risk Management** : Failure to correctly comply with RIPA could leave the Council exposed to investigation by the Interception Commissioner or legal action.

- Human Rights/  
Equalities/Diversity** : Complying with the Policy and Procedure will help to ensure compliance not just with RIPA, but also with Human Rights obligations, particularly Article 8 rights to private life.
- Equalities Impact  
Assessment** : The Policy and Procedure have both been assessed as applications to access communications data may impact on any individual citizens.
- Sustainability** : None arising from this report
- Environmental** : None arising from this report
- Social** : None arising from this report
- Economic** : None arising from this report
- Construction** : None arising from this report
- Signature** :

## **Main Considerations**

Council Services have had access to communications information for a number of years. Services utilise this information as an "investigatory tool" when exercising some statutory enforcement powers.

Since the coming into force of RIPA on 5<sup>th</sup> January 2004, there has been no formally adopted Policy or procedure to regulate a streamlined practice for applications of this nature across the organisation.

As a result of the Council's "Single Point of Contact" (SPoC), (a legal requirement to access communications information), retiring from employment in January 2007, a replacement had to be identified. The role of SPoC had historically been delegated to the Trading Standards Manager, who was appropriately trained and accredited by the Home Office. Having considered the costs involved with training a number of senior officers to be accredited, against the frequency with which the Council has used RIPA, alternative options were looked at. At present, negotiations are ongoing to conclude a contract with an external SPoC. This option is considered better value for money and will ensure that the Council always has a SPoC in place. Incidentally, Falkirk Council use the services of the external provider and have been pleased with the quality of Service received thus far.

The attached Policy and Procedure have been drafted to incorporate the application process used by the external SPoC. The procedure differs from the historical paper based application process in that data requests are completed on a secure on-line web based programme.

The Council may be subject to planned, or unplanned, inspections by the Interception Communications Commissioner, whose remit is to ensure that public authorities are adhering to the requirements of RIPA. A corporate overarching Policy and Procedure, together with specialised training programmes, would go some way to demonstrate the Council's commitment to compliance.

The Committee is requested to approve the Policy (Appendix 1) and Procedure (Appendix 2) as corporate guidance for accessing this type of information and is further requested to permit the City Solicitor to refine, if necessary, the Procedure for any further compliance once the external SPoC is in place.

**DRAFT**



**POLICY ON THE ACQUISITION AND DISCLOSURE  
OF COMMUNICATIONS DATA**

**under**

**Part1, Chapter 2 of the Regulation of Investigatory  
Powers Act 2000**

## **1. Introduction**

- 1.1 The access to, and use of communications data (information) has become a useful investigatory 'tool' for many public authorities. It has been used by local authorities along with the Police, Secret Services (MI5) and the Inland Revenue for a number of years. Sections 21-25 of the Regulation of Investigatory Powers Act 2000 (RIPA) came into force on 5<sup>th</sup> January 2004 and provided a statutory, human rights compliant, framework for obtaining communications data.
- 1.2 Communications data can be useful to a number of Council Services tasked with investigating alleged criminal activity as part of carrying out its statutory functions. For example, Sections such as CRM and Trading Standards may be required to investigate matters such as benefit fraud or consumer crime and being able to obtain this type of data may be crucial to the investigation.
- 1.3 Access to communications data is subject to a similar (but not identical) framework of authorisation, renewal and cancellation procedures, as that which exists for directed surveillance under the Regulation of Investigatory (Scotland) Act 2000 (RIPSA). For more information on RIPSA, see the City Solicitor's homepage.
- 1.4 As a matter of course, applications for access to this type of data should only be considered as a last resort and officers must have undertaken all necessary measures to obtain the desired information prior to seeking an authorisation under this Policy and accompanying Procedure.

## **2. Background**

- 2.1 The lawful acquisition of communications data by relevant public authorities<sup>1</sup> is governed by the Regulation of Investigations Powers Act 2000, Part 1, Chapter 2 (RIPA), which is applicable to the United Kingdom.
- 2.2 The powers to access communications data are set out in sections 21-25 of RIPA. The provisions of RIPA should be read in conjunction with the current statutory Code of Practice, which came into force on the 1st October 2007. The Code provides guidance on the procedures that require to be followed before access to communications data can occur and is admissible in court in criminal or civil proceedings.
- 2.3 Section 57 of RIPA provides that Prime Minister shall appoint an Interception of Communications Commissioner, who shall provide an independent oversight of the exercise and performance of the powers and duties contained within RIPA. The current Commissioner is the Right Honourable Sir Paul Kennedy and his appointment is from 11 April 2006 to 10 April 2009. RIPA also established an Independent Tribunal which has powers to investigate complaints submitted to it, anywhere in the United Kingdom. The Commissioner can make an award of compensation if he is of the view that an individual has been adversely affected by any wilful or reckless failure by any person within a relevant public authority in exercising or complying with the powers and duties inherent in RIPA.

---

<sup>1</sup> Regulation of Investigatory Powers (Communications Data) Order 2003

### **3. Objectives**

- 3.1 In some circumstances it may be necessary for Council employees, in the course of their duties, to require communications information about a person, either in their personal capacity or in the course of their trade or business. The acquisition of communications data under RIPA can be a justifiable interference with an individual's human rights, namely, the right to respect for private and family life inherent in Article 8 of the Human Rights Act 1998, only, where the conduct being authorised or required is determined to be necessary and proportionate and in accordance with the law.
- 3.2 ACC undertakes at all times to adhere to the requirements inherent in RIPA, the principles of good information handling within the Data Protection Act 1998, the practices set out in the statutory Code of Practice at the time, and premise of the Human Rights Act 1998.
- 3.3 In order to comply with its legal duties and responsibilities with respect to acquisition of communications data, ACC has adopted this policy together with a comprehensive procedure.

### **4. Procedure**

- 4.1 This Policy should be read in conjunction with the accompanying Corporate Procedure on the Acquisition and Disclosure of Communications Data. The Procedure shall be reviewed on an annual basis by the Office of the City Solicitor and shall take cognisance of any change within the law, further statutory guidance and any practice requirements as a result of a reported/ apparent ineffective practice or procedure being brought to the attention of City Solicitor.

### **5. Compliance**

- 5.1 Each Designated Person will be ultimately responsible for the non-adherence to this Policy by their officers. Where non-adherence by ACC officers is as a result of insufficient training, training needs must be addressed on an urgent basis.
- 5.2 Failure to correctly comply with this Policy and accompanying Procedure could leave ACC exposed to investigation by the Interception Communications Commissioner or legal challenge.
- 5.3 A breach of any of this Policy and Procedure by an officer is regarded by ACC an extremely serious matter and will be taken up by the Monitoring Officer. Depending upon the particular circumstances of the breach, such a matter may attract disciplinary proceedings against that member of staff. Where ACC staff deliberately and knowingly breach this Policy and Procedure, they will be subject to ACC disciplinary procedures, and such matter may be reported to the Police. All ACC staff can access details with respect to ACC disciplinary procedures directly from Human Resources, Resources Management.



# **PROCEDURE ON THE ACQUISITION AND DISCLOSURE OF COMMUNICATIONS DATA**

**under**

**Part1, Chapter 2 of the Regulation of Investigatory  
Powers Act 2000**



## Contents

Page No

1.	Introduction.....	3
2.	Definitions.....	3
3.	Principles.....	5
4.	The Application Process.....	6
5.	Data Request Fee.....	6
6.	Time period- Notices.....	7
7.	Renewals.....	7
8.	Cancellations.....	7
9.	Monitoring.....	8
11.	Security and the Retention of Records.....	8
11.	Data Protection.....	8
12.	Training.....	9
13.	Complaints.....	9
14.	Compliance.....	9
	<b>Appendix A- The Application Process.....</b>	<b>10</b>
	<b>Appendix B- The Web Form.....</b>	<b>11</b>
	<b>Appendix C- Refusal Notice.....</b>	<b>12</b>
	<b>Appendix D- Cancellation Notice .....</b>	<b>13</b>
	<b>Appendix E- Monitoring Record .....</b>	<b>14</b>
	<b>Appendix F- Investigatory Powers Tribunal contact details .....</b>	<b>15</b>

## 1. Introduction

- 1.1 This Procedure accompanies the Corporate Policy on the Acquisition and Disclosure of Communications Data and ensures that ACC is adhering to the requirements of RIPA when requesting and using communications data. Both the aforementioned Policy and this Procedure must be adhered to at all times.
- 1.2.1 RIPA provides for an Interception of Communications Commissioner whose remit is to provide an independent oversight of the exercise and performance of the powers contained within Part I of RIPA by organisations such as ACC. ACC may be subjected to inspections by the Commissioner on an unannounced basis at any time.
- 1.2.2 In the event of any queries about an application for a Notice, please contact the SPoC or the Office of the City Solicitor.

## 2. Definitions

**"ACC"**- means Aberdeen City Council

**"Collateral Intrusion"**- means the risk of the potential intrusion into the privacy of persons other than those who are the subjects of the investigation or operation.

**"Communications data"**- means;

- 1) any traffic data comprised in or attached to a communications (whether by sender or otherwise) for the purposes of any postal service or telecommunication system by means of which it is being or may be transmitted,
- 2) any information which does not include the contents of a communication (apart from anything falling within paragraph (a)) and is about the use made by any person –
  - (i) of any postal service or telecommunication service; or
  - (ii) in connection with the provision to or use by any person of any telecommunications service, of any part of a telecommunication system;
- 3) any information not falling within paragraph (a) or (b) 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.

**"CSP"**- means a Communications Services Provider.

**"Data Request"**- means the draft request completed by the Nominated Person.

**"Data Protection Act 1998"** An Act which makes provision for the regulation of the processing of information relating to individuals, including the obtaining, holding use or disclosure of such information.

- “Designated person”-** is an individual holding a position that satisfies the criteria laid down in the Schedule to the Regulation of Investigatory Powers (Communications Data) Order 2003, being a Head of Service, or an officer at third tier level who has designated powers to grant or refuse a request/Notice for communications data.
- “Nominated Person”-** means the Officer requiring the information for the purposes of their investigation.
- “Notice”-** is served on a CSP and requires the Operator/Service Provider to collect or retrieve the data requested and provide it to ACC.
- “RIPA”-** is the Regulation of Investigatory Powers Act 2000.
- “Service use data ”-** is information held by or obtained by a CSP, such as:
- Itemised telephone call records
  - Itemised connection records
  - Itemised timing and duration of calls
  - Connection/disconnection/reconnection data
  - Use of forwarding or redirection services
  - Additional telecom services
  - Records of postal items
- “ SPoC”-** means Singlepoint Data Services Limited.
- “Subscriber data”-** is information held by or obtained by a CSP about persons to whom the CSP provides or has provided a service, such as:
- Subscribers of e-mail and telephone accounts
  - Subscriber of a PO Box or Postage Paid Impression
  - Account information including payment details
  - Address for installing and billing
  - Abstract personal records (e.g. sign up data)
- “Web Form”-** is the form contained at Appendix A, that is completed by the Nominated Person using the E-Solution database accessible through the Internet by a secure log in.

### 3. Principles

In order to safeguard the Council from legal challenge, the interference with an individual's right to a private life, family, home and correspondence, by accessing communications information about that individual, must be justifiable and in accordance with the law. This means that the interference or 'access' must be both necessary and proportionate. The undernoted principles are inherent throughout the Web form and officers are required to establish and evidence both principles prior to the Designated Officer granting or refusing a Notice.

#### Necessity

- 3.1 RIPA provides that the conduct being authorised to take place requires to be both necessary and proportionate and in accordance with the law.
- 3.2 This Council is only permitted to access and use Service and Subscriber data, where it is necessary for the prevention and detection of crime or for preventing public disorder. No other use is permitted. Officers must demonstrate what crime, or potential crime may be committed and what statutory powers permit them to carry out that specific investigation .
- 3.2 In addition to the above, acquiring such data shall only be undertaken where there is no reasonable and effective alternative way of achieving the desired objective(s). If other options exist to secure the information without accessing communications data these must be considered and fully explored prior to an application being made under this procedure.
- 3.3 An application must be necessary at the time – it is not appropriate to seek authorisation for activities that may be necessary at some point in the future.

#### Proportionality

- 3.4 As well satisfying the statutory 'necessity' ground, officers also need to ensure that the conduct proposed is proportionate to the objective. For example, officers should consider the following prior to making a data request;
  - Is the conduct required proportionate to the outcome being sought to be achieved by obtaining the specified data?
  - Is it excessive?
  - Has every other possible means of investigation been exhausted?
  - Will the privacy of others, not the subject of the investigation, be affected?
  - How important is the data to the investigation?
  - How important is the investigation?
  - If ACC is unable to clearly demonstrate that the interference is justified, then the application should not proceed.
  - What is the likelihood of discovering confidential material?

#### Collateral Intrusion

- 3.5 Officers must have due regard to the possibility of intrusion into the lives of others who are not the subject of the investigation but whose information may be revealed. These may be other members of a household where an itemised list of calls will be obtained from a landline. The mere fact that collateral intrusion may occur does not

preclude a request or the grant of an Notice but parties should consider whether the risk of this is too high or whether steps can be taken to minimise this, the Web form should clearly demonstrate how any collateral intrusion will be managed.

## **4. The Application Process**

- 4.1 The Policy & Advice Team, Office of the City Solicitor, Resources Management, will provide each Nominated and Designated Person, with secure unique login details. The Office of the City Solicitor, as Monitoring Officer is responsible for maintaining an accurate record of Nominated and Designated Persons, and Services will be required to inform the City Solicitor should the list of Nominated and Designated Persons within their Service change.
- 4.2 Nominated Person(s) then log into 'E-Solutions' and submit a data request by completing the Web Form.
- 4.3 Web form must expressly detail the following:
  - a) statutory ground for the request
  - b) why it is considered proportionate in the circumstances
  - c) validity period of the notice
  - d) whether it is subscriber data or call data which is being requested
  - e) potential for collateral intrusion
  - f) the steps to be employed to minimise collateral intrusion
- 4.4 Upon receipt of the request, the SPoC will then check the request for accuracy to ensure what is being requested is lawful and that the CSP is identified and will, after being satisfied as to the competency and accuracy of the request, forward a Notice to the Designated Person.
- 4.5 The Designated Person will be informed by email correspondence that a Notice awaits to be authorised. The Designated Officer will then proceed to log into E-Solutions and shall determine whether the Notice be granted or refused. If granted, he/she advises the SPoC by email, who in turn sends the Notice to the CSP. The CSP will then send the information directly to the Nominated Person.
- 4.6 If the Designated Person refuses a Notice, he/she will advise the SPoC and the Nominated Person of his/her reasons and forward the Refusal Notice to the Office of the City Solicitor for recording. See Appendix C for a copy of the Refusal Notice.
- 4.7 A flowchart illustrating the process is available at Appendix A hereto.

## **5. Data Request Fee**

- 5.1 Each request for subscriber information attracts a Data Request Fee of £50.00. An additional fee of £10.00 may be payable, should the Nominated Person request assistance or consultation from the SPoC in relation to the completion of a data request.

- 5.2 The SPoC will forward an Invoice for the Data Request Fee (or other fee as agreed between the Service and the SPoC) to the Service requesting the data. The Invoice is payable within 30 days of receiving the Invoice for same and payment shall be by way of either an electronic transfer or cheque.
- 5.3 Failure of a Service to pay the Invoice within 30 days of receipt will render the Council in breach of contract.
- 5.4 Services will be required to note on the Monitoring Record (see Appendix D) whether an Invoice has been a) received and b) paid.

## **6. Time Periods – Notices**

- 6.1 A Notice expires after one calendar month beginning with the date on which it was granted by the Designated Person.
- 6.2 A Designated Person may specify a shorter time period if appropriate in the circumstances. Indeed, the Designated Person should specify the shortest period in which the objective for which the data is sought can be achieved. Where a notice relates to ‘future’ or ‘historical’ communications data, acquisition or disclosure of that data may only be required from the CSP **within** one month from the date upon which the authorisation was granted or notice given.

## **7. Renewals**

- 7.1 A request may be made for renewal of a Notice, at any time during the month it is valid, by the Nominated Person by completing a new Web form and forwarding it to the SPoC. The procedure is then the same as for a first request.
- 7.2 A renewed Notice takes effect at the point at which the previous Notice expires. A renewal Notice expires one calendar month from date it takes effect.
- 7.3 A Designated Person entitled to grant a Notice may grant or refuse a request for the renewal of the original Notice. A Notice may be renewed more than once, provided it continues to meet the criteria for Authorisation.

## **8. Cancellations**

- 8.1 A Designated Person shall cancel an Notice as soon as it is no longer *necessary*, or the conduct is no longer *proportionate* to what is sought to be achieved or the Notice has expired (whether having being renewed or not). The duty to cancel falls on the Designated Person that issued it.
- 8.2 If the request to a CSP for communications data involves future data or the request for historical data which has not yet been fulfilled, then a CSP will be notified by the SPoC that the Designated Person has cancelled the Notice.
- 8.3 On cancellation, the Cancellation form in Appendix D shall be forwarded to the Office of the City Solicitor and a copy retained by the Designated Person.

## **9. Monitoring**

- 9.1 Each Service shall maintain a record (see Appendix E) of all requests for acquisition of communications data (including refusals, renewals and cancellations of Notices) and shall forward that record to the Office of the City Solicitor at the end of each calendar month.
- 9.2 The Office of the City Solicitor shall maintain a central record of all requests, refusals, renewals and cancellations for the acquisition of communications data across the Council Service Areas and maintain an up to date list of those officers who have delegated powers to authorise Notices as Designated Persons and those who will be responsible for the use of such data as Nominated Persons.
- 9.3 Where any errors have occurred in the granting of any Notice a record should be kept, and a report and explanation sent to the Interception of Communications Commissioner as soon as is practical. Contact details are provided in Appendix F.

## **10. Security and Retention of Records**

- 10.1 The record referred to at 9.1 above is highly confidential and must be treated as such. Services shall make proper arrangements for their retention, security and destruction, in accordance with the requirements of the Data Protection Act 1998 and Aberdeen City Council's 'Corporate Data Protection Policy' and accompanying procedures.
- 10.2 The Designated Person shall pass all supporting documents pertaining to requests, renewals, refusals and cancellations to the City Solicitor. Copies of the Central Record shall be retained for three (3) years from the date of the Notice, cancellation, refusal or renewal. These copies will be kept in a secure and locked cabinet at all times and access to the cabinet should be restricted to the Designated Person or Chief officers.
- 10.3 The Office of the City Solicitor will undertake an audit of requests made under RIPA on an annual basis, in conjunction with the Audit for Covert Surveillance under the Regulation of Investigatory Powers (Scotland) Act 2000.
- 10.4 Upon expiry of the retention period referred to in 10.2 above, any documentation unless required or potentially required for any proceedings or Appeal, documents must then be disposed of in a secure manner.

## **11. Data Protection**

- 11.1 Officers will have regard to the provisions of the Data Protection Act 1998 in relation to communications data retained by it as a result of an application to access communications data. In particular, officers recognise that the subject of the investigation/ operation can has a right to access information held about them which includes communications data obtained and held by ACC for business purposes. Should a request be received for communications data, officers should seek advice

from their Service Data Protection Liaison Officer (DPLO). An up-to-date list of DPLOs can be found in the City Solicitor's homepage.

## **12. Training**

- 12.1 The Office of the City Solicitor will be responsible for training Nominated and Designated Persons with respect to the use and completion of the Web Form on the E-Solution online system, as and when required. All requests for training from Services should be made directly to the Legal Manager of the Policy and Advice Team.
- 12.2 It is a requirement that Nominated and Designated Persons attend training prior to either submitting or authorising a data request for communications data.

## **13. Complaints**

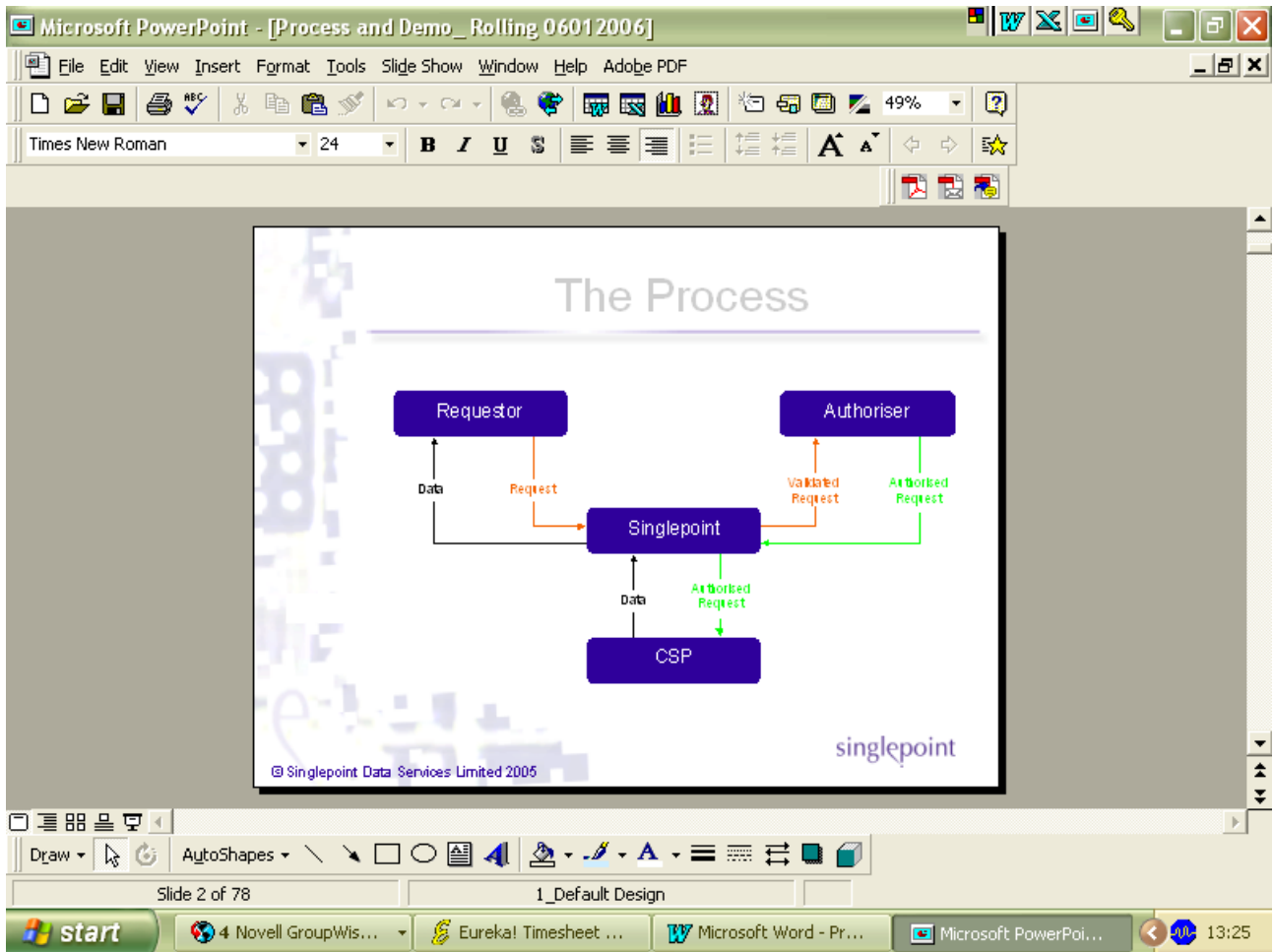
- 13.1 RIPA establishes an independent Tribunal, which is made up of senior members of the legal profession or judiciary and is independent of the Government. The Tribunal has full powers to investigate and decide any case within its jurisdiction.
- 13.2 If a member of the public wishes to complain in relation to the acquisition of communications data associated with them, then a complaint can be made in accordance with the Council's Corporate Complaints Procedure or the individual can contact the Investigatory Powers Tribunal separately. Please see Appendix E for contact details.

## **14. Compliance**

- 14.1 Both Nominated and Designated Persons are required to adhere to this procedure when making requests for communications data. Failure to do so may result in a complaint being made and investigated by the Interception Communications Commissar of the Investigatory Powers Tribunal, or may result in ACC being subject to legal challenge, should any evidence it relies upon in any legal proceedings have been gathered unlawfully.
- 14.2 Any breach of this Procedure by an officer is regarded by ACC an extremely serious matter and will be taken up by the Monitoring Officer in the first instance.



## Appendix A- The Application Process.



Please note the following definitions referred to above:

"Requestor" = the Nominated officer  
"Authoriser" = the Designated Officer


## Appendix B- The Web Form

Request Form - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Back Forward Stop Refresh Home Search Favorites Print Mail Stop

Address <https://www.singlepointdataservices.org/spds/servlet/newRequest>

**Secure access** Data request form 

**Requestor** [log-out](#) | [secure home page](#) | [legislation overview](#) | [help](#)

**NOTICE REQUIRING DISCLOSURE OF COMMUNICATION DATA**  
**(Under section 22(4) of the Regulation of Investigatory Powers Act 2000)**

**REQUEST SECTION**

Requestor ID	<input type="text" value="do81ja"/>
Requestor Name	<input type="text" value="Jane Doe"/>
Authority	<input type="text" value="Anytown Council"/>
Address	<input type="text" value="Town Hall"/>
Address (Cont'd)	<input type="text" value="Station Road"/>
City	<input type="text" value="Anytown"/>
County	<input type="text" value="Anycounty"/>
Postcode	<input type="text"/>
Contact Telephone Number	<input type="text" value="087000 56474"/>
Contact Mobile Number	<input type="text"/>
Contact Fax Number	<input type="text" value="087000 56475"/>
Date	<input type="text" value="03/06/2005"/>
Type of Request	<input type="text" value="To obtain communications data"/> ▼
Priority	<input type="text" value="Low"/> ▼









## **Appendix F- Investigatory Powers Tribunal**

The Act established an independent Tribunal ('the Investigatory Powers Tribunal'). The Tribunal is made up of senior members of the judiciary and the legal profession and is independent of the Government. The Tribunal has full powers to investigate and decide any case within its jurisdiction which includes the acquisition and disclosure of communications data under the Act.

The Tribunal can investigate anything an individual believes has taken place against him/her, his/her property or communications, as long as it relates to a power held by the organisation you are complaining about, under the Regulation of Investigatory Powers Act.

The Tribunal can be contacted by post on:

The Investigatory Powers Tribunal  
PO Box 33220  
London  
SW1H 9ZQ  
Tel: 0207 035 3711

Or visit the website:  
<http://www.ipt-uk.com/>