Agenda Item No: 3

REVISED POLICY IN RELATION TO THE REGULATION OF INVESTIGATORY POWERS ACT 2000

To:	**Constitution and Ethics Committee**
Meeting Date:	**27th February 2018**
From:	**LGSS Director of Law & Governance and Monitoring Officer**
Electoral division(s):	**All**
Purpose:	**For the Committee to consider the revised policy for the Council's obligations under the Regulation of Investigatory Powers Act 2000 (RIPA).**
Recommendation:	**That the Committee endorse and adopt the revised Regulation of Investigatory Powers Act (RIPA) Policy as a formal record of the Council's use of and compliance with RIPA**.

	Officer contact:
Name:	Quentin Baker
Post:	Director of Law and Governance and Monitoring Officer; Director of LGSS Law Ltd.
Email:	Quentin.Baker@LGSSLaw.co.uk
Tel:	01223 727 961

1. BACKGROUND

1.1 The Regulation of Investigatory Powers Act 2000 (RIPA) provides a statutory framework regulating the use of directed surveillance and the conduct of covert human intelligence sources (informants or undercover officers) by public authorities. The Act requires public authorities, including local authorities, to use covert investigation techniques in a way that is necessary, proportionate and compatible with human rights. RIPA also provides for the appointment of a Chief Surveillance Commissioner to oversee the way in which public authorities carry out covert surveillance.

1.2 RIPA governs the acquisition and disclosure of communications data and the use of covert surveillance by local authorities. The Council uses powers under RIPA to support its core functions for the purpose of prevention and detection of crime where an offence may be punishable by a custodial sentence of six months or more, or is related to the underage sale of alcohol and tobacco.

1.3 The three powers available to local authorities under RIPA: the acquisition and disclosure of communications data; directed surveillance; and covert human intelligence sources ("CHIS"). The Act sets out the procedures that Cambridgeshire County Council must follow if it wishes to use directed surveillance techniques or acquire communications data in order to support core function activities (e.g. typically those undertaken by Trading Standards, Environmental Health and Benefits). The information obtained as a result of such operations can later be relied upon in court proceedings providing RIPA is complied with.

1.4 The Home Office Code for Covert Surveillance Property Interference recommends that elected members, whilst not involved in making decisions or specific authorisations for the local authority to use its powers under Part II of the Act, should review the Council's use of the legislation and provide approval to its policies.

1.5 The revised Cambridgeshire County Council RIPA Policy is attached at **Appendix** 1.

2. MAIN ISSUES

2.1 Updated RIPA Policy

2.1.1 The Cambridgeshire County Council RIPA Policy has been reviewed and updated in line with the Commissioner's recommendations and to reflect the increasing availability of social media web sites for potential research or intelligence gathering.

2.1.2 Policy is publicised internally on an annual basis around the same time as the annual report. This will serve to remind officers of the possible uses for RIPA but also remind officers of the circumstances when a RIPA authorisation is required.

Source Documents	Location
Regulation of Investigatory Powers Act (2000)	http://www.legislation.gov.uk/ukpga/2000/23/contents

Appendix 1

The Regulation of Investigatory Powers Act 2000 (RIPA)

A POLICY & PROCEDURE GUIDE

On the use of covert surveillance and covert human intelligence sources

---

CONTENTS

PART I

THE GUIDE TO RIPA

1. Introduction

1.1. This Guide sets out the Council's obligations under the Regulation of Investigatory Powers Act 2000 (RIPA). RIPA requires the Council to have in place procedures which ensure that where required, surveillance is necessary, proportionate and properly authorised.

1.2. The Council takes its statutory responsibilities seriously and will, at all times, act in accordance with RIPA and the Codes of Practice and take necessary and proportionate actions in these matters.

2. Cambridgeshire County Council's Policy

2.1. Having regard to the above, the Council's Policy for the conduct of covert surveillance is :-

2.1.1. Cambridgeshire County Council shall only undertake covert surveillance of a private individual in accordance with the provisions of RIPA.

2.1.2. The Council and its Officers shall only carry out surveillance where it is reasonably believed that the authorisation is necessary for the purposes of preventing and detecting crime or preventing disorder. The Council shall ensure that the surveillance is proportionate to what it seeks to achieve.

2.1.3. It is a requirement of this Policy that all officers involved in RIPA processes receive full and appropriate training.

3. Background – What does RIPA do?

3.1. RIPA sets out the statutory mechanism for authorising covert surveillance, the use of a Covert Human Intelligence Source (CHIS) and the acquisition of communications data. It seeks to ensure that any interference with a citizen's rights under Article 8 of the European Convention and the Human Rights Act 1998 is necessary and proportionate and therefore there is a proper balance between the public interest and the human rights of individuals.

3.2. Some Council activities may necessarily require covert surveillance to be used in the course of its statutory enforcement functions, for example, benefit fraud, fly-tipping, schools, planning or licensing enforcement.

3.3. Surveillance is a last resort that an investigator will utilise to prove or disprove an allegation. Covert surveillance must only be undertaken where there is no reasonable and effective alternative means of achieving the desired objective. No activity shall be undertaken within the definition of intrusive surveillance

4. The Rules

4.1. All employees of the Council and external agencies working for the Council are covered by RIPA and Human Rights Act 1998 whilst they are working for the Council.

4.2. It is crucial that all directed surveillance is properly authorised and prior approval has been obtained from the Magistrates' Court.

4.3. Any evidence gathered by surveillance subject to RIPA but not properly authorised may be inadmissible in court. Surveillance without proper authorisation could also lead to complaints, challenges and/or claims for compensation. Therefore, it is essential that all involved with RIPA comply with this Guide and procedure.

4.4. The Council **can only** authorise use of directed surveillance under RIPA to prevent or detect serious criminal offences that are either punishable by at least 6 months' imprisonment or more **or** are related to the underage sale of alcohol and tobacco.

4.5. The Council **cannot** authorise directed surveillance for the purpose of preventing disorder (unless this involves a criminal offence(s) punishable with of at least 6 months' or more imprisonment e.g. criminal damage, dangerous waste dumping);

4.6. The Council **can only** authorise the use of directed surveillance provided that the tests of necessity and proportionality are met. In other words if you can carry out an investigation by means which do not involve directed surveillance, then you cannot demonstrate surveillance is necessary and you must use those alternative means over surveillance.

4.7. The Council **cannot** carry out intrusive surveillance.

4.8. The Council is subject to audit and inspection by the Office of the Surveillance Commissioner, which oversees the conduct of covert surveillance and covert human intelligences sources by public authorities in accordance with legislation. It is important that the Council demonstrates compliance with RIPA and with this Policy.

4.9. *What is not covered*

4.9.1. Most surveillance carried out by the Council will be overt and not covert. Officers in doing their normal jobs, for example, inspection of food premises, where the subject knows about the inspection will be carrying out overt surveillance. Overt surveillance does not require authorisation under RIPA.

4.9.2. Other examples would be an officer may be on duty at public events and will monitor the crowd to maintain public safety and prevent disorder; Environmental

Health Officers might covertly observe and then visit a shop as part of their enforcement function. Such observation may involve the use of equipment merely to reinforce normal sensory perception, such as binoculars, or the use of cameras, where this does not involve systematic surveillance of an individual. It forms a part of the everyday functions of law enforcement or other public bodies.

4.9.3. The provisions of the Act do not cover the use of overt CCTV surveillance systems or Automatic Number Plate Recognition Cameras (ANPR). Members of the public are aware that such systems are in use, for their own protection, and to prevent crime. Their operation is covered by the Data Protection Act 1998 and the CCTV Code of Practice 2008, issued by the Information Commissioner's Office. Similarly, the overt use of ANPR systems to monitor traffic flows or detect motoring offences does not require an authorisation under RIPA. For information about this, contact Rob Lawrence, CCTV Team Leader, or the Council's Senior Responsible Officer (SRO) or the RIPA Co-Ordinator (whose contact details are in Part II of this document.)

4.9.4. However, where overt CCTV or ANPR cameras are used in a covert and pre-planned manner as part of a specific investigation or operation, for the surveillance of a specific person or group of people, a directed surveillance authorisation must be considered. Such covert surveillance is likely to result in the obtaining of private information about a person (namely, a record of their movements and activities) and therefore falls properly within the definition of directed surveillance.

4.10. *What is covered*

4.10.1. The Act is designed to regulate the use of "covert" surveillance which is directed surveillance, Intrusive Surveillance and the use of a CHIS. These are dealt with individually below. It also permits the Council to compel disclosure of communications data from telecom and postal companies or obtain communications records from communications companies.

5. Types Of Surveillance

5.1. "Covert Surveillance"

5.1.1. This is defined as "surveillance which is carried out in a manner calculated to ensure that the persons subject to the surveillance are unaware that it is or may be taking place" It should be noted that surveillance may also intrude on the privacy of others who are not the subject of surveillance but who are unintentionally observed.

5.2. "Directed Surveillance" is surveillance which is

5.2.1.1. covert; and

5.2.1.2. not intrusive (as defined below); and

5.2.1.3. not carried out as an immediate response to events which would otherwise be unreasonable to seek authorisation e.g. seeing something suspicious and continuing to observe it; and

5.2.1.4. undertaken for the purpose of a specific investigation or operation; and

5.2.1.5. in a manner likely to obtain private information about an individual (whether or not that person is specifically targeted for the purposes of an investigation).

5.2.2. The key issue in "Directed Surveillance" is the targeting of an individual with the likelihood of gaining private information. Private information in relation to a person includes any information relating to his/her private or family life to produce a detailed picture of a person's life, activities and associations.

5.2.3. In practice, the sort of directed surveillance which the Council might undertake would include the use of concealed cameras as part of an investigation into antisocial behaviour, it might include covert surveillance connected with the enforcement of environmental health regulations or in connection with investigating benefit fraud.

5.2.4. You must treat anything involving the use of concealed cameras or anything involving keeping covert observation on premises or people as potentially amounting to directed surveillance. If you are unsure, please take advice either from your manager or supervisor, or from the RIPA Co-Ordinator within LGSS.

5.2.5. Directed surveillance **must** be properly authorised in accordance with the procedure set out from paragraph 7 onwards.

5.2.6. You must treat any covert surveillance which is likely to intrude upon anyone's privacy to more than a marginal extent as directed surveillance, even if it does not fall within the strict terms of the definition – for instance where surveillance is not part of a specific investigation or operation.

5.3. *Directed Surveillance and Social Media*

5.3.1. Viewing of open source material on the internet does not require authorisation **unless and until** it is repeated or systematic, at which stage directed surveillance authorisation should be considered. If your proposed use of the internet or social media (whether as part of a formal investigation or otherwise) amounts to covert directed surveillance within the scope of RIPA by electronic means, an authorisation is needed in accordance with the procedure set out from paragraph 7 onwards.

Whenever you intend to use the internet as part of an investigation, you must first consider whether the proposed activity is likely to interfere with a person's Article 8 rights, including the effect of any collateral intrusion and must only be used when necessary and proportionate to meet the objectives of a specific case.

Passing an access control so as to look deeper into an internet site or social media, for example by making a "friend request", requires at least directed surveillance authorisation. If the investigation is to go further and pursue enquiries within the site, thereby establishing a relationship with the site host in the guise of a member

of the public, this requires a CHIS authorisation and the SRO or RIPA Co-Ordinator must be consulted.

5.3.2. Where individuals publish information freely (e.g. twitter accounts, LinkdIn profiles), this may not amount to an interference with Article 8 rights. However, care should be taken with other social media, such as Facebook. Even if the user has not used privacy settings to restrict access, this does not necessarily mean that they have made a decision to publish personal information to the world. Therefore if you are considering monitoring social media such as Facebook in connection with an investigation, you must first seek advice on whether RIPA authorisation is needed.

5.4. "Intrusive Surveillance"

WARNING:
THE COUNCIL CANNOT CARRY OUT INTRUSIVE SURVEILLANCE.

Intrusive surveillance is defined as:

5.4.1.1. Covert surveillance; and

5.4.1.2. is carried out in relation to anything taking place on any residential premises or in any private vehicle; and

5.4.1.3. involves the presence of a person on the premises or in a vehicle or is carried out by a surveillance device in the premises or vehicle.

5.4.2. In essence, intrusive surveillance amounts to intrusion into people's homes or vehicles either physically or by means of a surveillance device.

5.4.3. Surveillance equipment mounted outside the premises or vehicle will not be intrusive, unless the device consistently provides information of the same quality and detail as might be expected if they were in the premises or vehicle. High quality video or CCTV cameras may run the risk of providing high quality data which may be considered intrusive. Similarly some recording devices used to record noise may provide evidence of the same quality as if the device was actually in the premises. Care must be taken to properly assess whether the information will be intrusive. If officers are in any doubt they must seek advice from the RIPA Co-Ordinators.

5.4.4. Intrusive surveillance can only be carried out by the police and other specific law enforcement agencies like Customs and Excise. **The Council cannot authorise intrusive surveillance and cannot carry out intrusive surveillance.** If you are asked by another agency to co-operate with intrusive surveillance, you must seek advice from SRO or the RIPA Co-Ordinator immediately. Where other authorities say that they are authorised to undertake intrusive surveillance but need our co-operation, we need to check their authorisation.

5.5. A "Covert Human Intelligence Source" (CHIS) is defined as:

5.5.1.1. a person who establishes or maintains a relationship with another person for the covert purpose of EITHER:

5.5.1.2. covertly using such a relationship to obtain information or to provide access to any information to another person;

OR

5.5.1.3. they covertly disclose information obtained by the use of such a relationship or as a result of the existence of such a relationship;

5.5.2. The key issue is the relationship is conducted in a manner that is calculated to ensure that one of the parties to the relationship is unaware of its purpose or (in the case of disclosure of information) it is disclosed in a manner that is calculated to ensure that one of the parties to the relationship is unaware of the disclosure in question.

5.5.3. Persons who complain about Anti-Social Behaviour and are asked to keep a diary will not normally be CHIS as they are not required to establish or maintain a relationship for a covert purpose. However, if we are relying on, say, a neighbour to ask questions with a view to gathering evidence, then this may amount to use of a covert human intelligence source and authorisation must be sought.

5.5.4. A young person carrying out a single test purchase at a shop would not normally be considered to be a CHIS, however if the young person revisits the same shop so as to encourage familiarity, they could be considered a CHIS and authorisation must be sought.

5.5.5. The use by the Council of CHIS is expected to be extremely rare and, for that reason, this guide does not deal with the issues to which they give rise. If you are contemplating use of a covert human intelligence source, please take specific advice from the RIPA Co-Ordinator before putting your plan into action. There are a number of arrangements that need to be in place before a CHIS can be used, such as the appointment of an officer who is responsible for welfare and security of the CHIS.

5.6. Communications Data

5.6.1. The provisions of RIPA permit local authorities to access communications data where it is necessary for the purpose of preventing or detecting crime.

5.6.2. There are stringent controls placed on access by the Council to "communications data". The Council is not entitled to obtain access to the content of communications between third parties but can, in some circumstances, obtain information relating to the use of a communications service. "Communications services" include telecom providers, postal services and internet service providers.

5.6.3. This is a complex area, procedurally and legally. Access to communications data can only be obtained through the Council's designated "single point of contact" ("SPOC") for communications data

5.6.4. Communication data means any traffic or any information that is or has been sent by or over a telecommunications system or postal system, together with information about the use of the system made by any person.

5.6.5. These powers must be used in accordance with the Code of Practice on Accessing Communications.

If you wish to use access communications data, only the SRO, [[insert] Designated Persons at the Council for the purpose of Communication Data. You must speak to the Designated Personsor the RIPA Co-Ordinator to access communications data.

The designated person shall consider the application and record his/her considerations at the time in writing or electronically. If the application is necessary and proportionate in the circumstances, an authorisation is granted. The 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.

Designated persons must ensure that they grant authorisations or give notices only for purposes and only in respect of types of communications data that a designated person of their position in the Council may grant or give. The designated person shall take account of any advice provided by the SPoC.

Designated persons should not be responsible for granting authorisations or giving notices in relation to investigations or operations in which they are directly involved.

5.7. Legally Privileged, Religious Material and Confidential Information

5.7.1. Particular care must be taken in cases where the subject of the investigation or operation might reasonably expect a high degree of privacy, or where confidential information is involved. Confidential information consists of communications subject to legal privilege, communications between a Member of Parliament and another person on constituency matters, confidential personal information, or confidential journalistic material. It can include medical or financial records.

5.7.2. It is unlikely that the normal surveillance activities of the Council will result in acquisition of this type of information but where the risk analysis identifies a possibility of obtaining such information prior consultation with the RIPA Co-Ordinator must be carried out who will also discuss it with the SRO. If confidential information is or is likely to be obtained the Chief Executive must specifically authorise the surveillance. It will require particularly strong justification and arrangements will need to be put in place to ensure that the information obtained is kept secure and only used for proper purposes.

6. Codes of Practice

6.1. Codes of practice exist for all areas of RIPA including Covert Surveillance, Covert Human Intelligence Sources and Acquisition and Disclosure of Communications Data. There is also guidance for surveillance camera system or CCTV operators. These Codes are not reproduced in this Guide because they are subject to change, updating and amendments. However the Codes together with other information on RIPA can be accessed via http://surveillancecommissioners.independent.gov.uk which is the Office of Surveillance Commissioners' website.

6.2. Officers using RIPA must be familiar with the Codes of Practice.

7. Authorising Directed Surveillance

7.1. Detailed guidance on the authorisation procedure and on how to complete the statutory forms is available on the Council's Intranet.. . You must only use the forms that are on the Intranet, you must read the accompanying notes carefully and follow them when completing the form.

7.2. *Who can authorise directed surveillance?*

7.2.1. Regulations made under the Act say that the most junior level at which authorisations can be given is by what it refers to as "assistant chief officers". For the purposes of this Code, authorisations may only be given by the officers identified in Part II of this Guide referred to as "authorising officers". They must have received appropriate training.

7.2.2. Where practical, the authorising officer must not be directly involved in the case giving rise to the request for authorisation. (However, an authorising officer may authorise a request made by staff who report to them if they are not directly involved in the case.) Where it is not practical for authorisation to be given by an officer who is not directly involved, this must be noted with reasons on the authorisation form.

7.2.3. In addition to internal authorisation, directed surveillance cannot be carried out without the approval of a Magistrate. (See paragraph 8 below)

7.3. *On what grounds can directed surveillance be authorised?*

7.3.1. As mentioned, the Council can only authorise directed surveillance if it is **necessary** and **proportionate** and for certain purposes, namely to prevent or detect serious criminal offences that are either punishable by at least 6 months' imprisonment or more or are related to the underage sale of alcohol and tobacco.

7.4. *Is the proposed surveillance proportionate?*

7.4.1. Authorisation cannot be sought, and authority must not be given unless you are satisfied that the surveillance is proportionate. You have to make sure that any interference with privacy is justified by the end being sought. Unless the benefit to

be obtained from surveillance is significant, and unless the problem you are seeking to tackle is serious, the use of surveillance is unlikely to be proportionate.

7.4.2. In assessing proportionality, consider whether other less intrusive means could be used to gather information.

7.4.3. Take into consideration the risk of intrusion into the privacy of persons (including those not subject to the investigation).

7.4.4. You should ask is the proposed surveillance discriminatory? The Council is under a legal obligation to avoid either direct or indirect discrimination in carrying out its functions. As surveillance can interfere with rights contained in the European Convention on Human Rights, discrimination can also amount to a breach of the Human Rights Act. You should be sensitive to this issue and ensure that you apply similar standards to seeking or authorising surveillance regardless of ethnic origin, sex or sexual orientation, disability, age etc. You should be alert to any assumptions about people from different backgrounds which may not even be consciously held. Consider the diverse impact on community confidence that may result from the information obtained.

7.5. *Consider the degree of intrusion for those likely to be affected*

7.5.1. In other words, might the surveillance intrude upon the privacy of people other than those who are the subject of the investigation? This is known as collateral intrusion. You must be sensitive of the privacy rights of third parties and consider very carefully whether the intrusion into their privacy is justified by the benefits of undertaking the surveillance. Consider if there are measures that can be put in place to avoid any collateral intrusion.

7.6. The Procedure

7.6.1. Before submitting an application for authorisation, you must supply a copy of your request to the SRO or RIPA Co-Ordinator. The RIPA Co-Ordinator will provide a Unique Reference Number for each RIPA application, upon request by an Investigating Officer. The RIPA Co-Ordinator can provide advice and assistance to the Investigating Officer and the Authorising Officer. You may only submit your application for authorisation if you obtain the approval of the SRO or RIPA Co-Ordinator.

7.6.2. A written application for authorisation for directed surveillance must describe in detail any conduct to be authorised and the purpose of the investigation or operation. The application shall also include:

7.6.2.1. A description of the nature of the surveillance;
7.6.2.2. the identities, where known, of those to be the subject of the surveillance;
7.6.2.3. an explanation of the information which it is desired to obtain as a result of the surveillance;
7.6.2.4. the reasons why the authorisation is necessary in the particular case
7.6.2.5. and on the grounds (e.g. for the purpose of preventing or detecting crime) listed in Section 28(3) of the 2000 Act;

7.6.2.6. the reasons why the surveillance is considered proportionate to what it seeks to achieve;
7.6.2.7. the details of any potential collateral intrusion and why the intrusion is justified;
7.6.2.8. the details of any confidential information that is likely to be obtained as a consequence of the surveillance.

7.6.3. A subsequent record is needed of whether authority was given or refused, by whom and the time and date.

7.6.4. In assessing an application the Authorised Officer must also be mindful of corporate policy and satisfy himself or herself that the RIPA authorisation is in accordance with the law, necessary and proportionate.

7.6.5 When authorising the conduct or use of CHIS the Authorised Officer must also be satisfied that the conduct and/or use of the CHIS is proportionate to what is being sought to be achieved. They must also be satisfied that the appropriate arrangements are in place for the management of the CHIS. This must include a risk assessment for health and safety.

WARNING: Ensure that records are available on a need to know basis.

8. Authorisation by the Magistrates' Court

8.1. Prior to any directed surveillance being carried out, the Council is required to apply for approval from the Magistrates' Court and until such approval is in place, you must **not** commence your surveillance.

8.2. Once the application for authorisation is approved by an Authorising Officer and the SRO or RIPA Co-Ordinator, the Co-Ordinator will make arrangements for application to be made to the Magistrates' Court to obtain the approval of every authorisation or renewal that has been granted. The Co-Ordinator will obtain details of the relevant Authorising Officer when providing a Unique Reference Number and will require the Authorising Officer to provide the original signed authorisation or renewal that has been granted as soon as reasonably practicable, in order that an application may be made to the Magistrates' court in good time.

8.3. The Co-Ordinator will advise the relevant Authorising Officer and the relevant Investigating Officer as soon as reasonably practicable of the outcome of the application to the court for approval of the authorisation.

8.4. A Magistrate may only approve the application if satisfied that it:

8.4.1. is necessary for the purposes set out in RIPA and is proportionate in human rights terms to what it seeks to achieve;
8.4.2. has been authorised by a person in the Council at the level designated in RIPA;
8.4.3. meets any other restriction imposed (for example the 'serious crime' threshold that applies to directed surveillance); and
8.4.4. sets out, for CHIS's, that the relevant procedures and supporting officers are in place to protect the welfare and safety of the CHIS.

9. Time Limits & Cancellations

9.1. The authorisation must be reviewed within the time stated on the application form and cancelled by the authorising officer who authorised it if no longer necessary.

9.2. **WARNING: there must be a cancellation form completed for each authorisation once surveillance is completed**. In other words it cannot be left to simply lapse. A copy of the form must be given to the SRO.

9.3. The authorisation for directed surveillance will cease to have effect (unless renewed or cancelled) at the end of **3 months** from the date on which the authorisation takes effect (and 12 months for a CHIS).

10. Reviews

10.1. Regular reviews of authorisations must be undertaken to assess the need for the surveillance to continue. The maximum period between authorisation and review, and between reviews, is **four weeks.** The more significant the infringement of privacy, the more frequent the reviews. The results of a review must be recorded on the central record of authorisations. Particular attention is drawn to the need to review authorisations frequently where the surveillance provides access to confidential information or involves collateral intrusion.

10.2. In each case authorising officers within the Council shall determine how often a review will take place. This must be as frequently as is considered necessary and practicable.

10.3. A link to the form to record a review of an authorisation may be found in [to be inserted].

11. Renewals

11.1. If at any time before an authorisation would cease to have effect, the authorising officer considers it necessary for the authorisation to continue for the purpose for which it was given, s/he may renew it in writing for a further period of **three months**. A renewal cannot take effect unless it has been approved by a Magistrate. If you think a renewal might be needed, you need to plan to allow sufficient time for an application to a Magistrate to be made before expiry.

11.2. A renewal takes effect at the time at which, or day on which the authorisation would have ceased to have effect but for the renewal. An application for renewal is not to be made until shortly before the authorisation period is drawing to an end. Any person who would be entitled to grant a new authorisation can renew an authorisation. Authorisations may be renewed more than once, provided they continue to meet the criteria for authorisation.

11.3. All applications for the renewal of an authorisation for directed surveillance must be made on the form and must record:

11.3.1. whether this is the first renewal or every occasion on which the authorisation has been renewed previously;

11.3.2. any significant changes to the information given in the original application for authorisation;
11.3.3. the reasons why it is necessary to continue with the directed surveillance;
11.3.4. the results of regular reviews of the investigation or operation.

11.4. Authorisations may be renewed more than once, if necessary, and the renewal must be kept/recorded as part of the central record of authorisations (see paragraph155).

11.5. In addition, the Co-Ordinator will review and comment upon each authorisation/renewal before it is made by the Authorising Officer to ensure that such authorisations/renewals are granted properly, are appropriate and that all forms have been fully completed.

12. Monitoring

12.1. Quentin Baker, LGSS Director of LGSS Law, is the Council's appointed Senior Responsible Officer for RIPA. He has responsibility for the integrity of the process to authorise directed surveillance, to ensure compliance with the Act and the Codes of Practice, to engage with the Commissioners and Inspectors when they conduct inspections, to oversee the implementation of any post-inspection action plan recommended or approved by a Commissioner and to ensure all Authorising Officers are of an appropriate standard.

12.2. The Senior Responsible Officer will provide an annual report to the General Purposes Committee to enable continual Member oversight of this RIPA Policy, to provide a summary of operations, training and central records concerning the Council's use of RIPA powers.

12.3. The SRO maintains this Policy and Guide on behalf of the Council, ensuring it is up to date and accurate. The SRO must also maintain a central record of authorisations and maintain a list of authorised officers for the purpose of RIPA.

12.4. Regular monitoring of authorisations shall be undertaken by the SRO to ensure compliance with RIPA, the Codes of Practice and Council Policy. In addition, as part of the democratic process, elected Members review the use of RIPA powers by the Council. This process is administered through the Council's Constitution.

12.5. In cases where the Council is acting on behalf of another authority or agency (e.g. the Police) the other authority normally obtain or provide the authorisation. In cases where the Council is the lead authority it will obtain the required authorisation and where operational support of other agencies is foreseen, this must be specified in the authorisation.

13. Errors

13.1. Any errors must be reported to the SRO and advice sought on what action is needed.

14. Disclosure and Retention Of Material

14.1. Material obtained from a source may be used as evidence in criminal proceedings. The proper authorisation of a source will ensure the suitability of such evidence and compliance under the common law, Section 78 of the Police and Criminal Evidence Act 1984, the Data Protection Act 1998 and the Human Rights Act 1998. Furthermore, the product or information obtained by a source is subject to the ordinary rules for retention and disclosure of material under the Data Protection Act 1998 and Criminal Procedure and Investigations Act 1996. There are well established legal procedures that will protect the identity of a source from disclosure in such circumstances.

15. Keeping Of Records

15.1. A record of the following information pertaining to all authorisations shall be held centrally and retrievable for a period of three years from the ending of each authorisation. This information must be regularly updated whenever an authorisation is granted, renewed or cancelled.

- a copy of the application and a copy of the authorisation together with any supplementary documentation and notification of the approval given by the authorising officer
- a record of the period over which the surveillance has taken place
- the frequency of reviews prescribed by the authorising officer
- a record of the result of each review of the authorisation
- a copy of any renewal of an authorisation, together with the supporting documentation submitted when the renewal was requested
- the date and time when any instruction to cease surveillance was given
- the date and time when any other instruction was given by the authorising officer.

A copy of all completed forms authorising, renewing or cancelling directed surveillance must be provided to the SRO.

Pursuant to the Council's Constitution I approve the amendments to the Council's Policies and Procedures regarding the Regulation of Investigatory Powers Act 2000 as contained in this Guide.

Signed:

Quentin Baker
Assistant Director Legal & Democratic Services and Monitoring Officer