APPENDIX 2

CORPORATE POLICY AND PROCEDURE ON THE REGULATION OF INVESTIGATORY POWERS ACT 2000

Introduction

1. The Regulation of Investigatory Powers Act 2000 (**RIPA**) is concerned with the regulation of surveillance and other intelligence gathering by public authorities in the conduct of their legitimate business. These activities are an unavoidable part of modern public life, but only in recent years have they been made the subject of formal statutory control.

2. Section 6 of the Human Rights Act 1998 provides that it is unlawful for a public authority to act in a way which is incompatible with a European Convention right. Article 8 of the European Convention of Human Rights says that everyone has the right to respect for their private and family life, their home and their correspondence.

3. The use of surveillance and other intelligence gathering techniques may amount to an interference with rights protected by Article 8 of the European Convention and could amount to a violation of those rights unless the interference is in accordance with the law.

4. RIPA was enacted to ensure these activities do not infringe the Human Rights Act by establishing a statutory framework which is consistent with the European Convention and by introducing national standards which are applicable to all public authorities.

5. The Council has approved a policy for tackling fraud and corruption. In limited circumstances the Council may wish to use surveillance techniques for the purpose of enforcing this policy or other of its statutory functions. The requirements of RIPA are most likely to apply to those Sections of the Council with enforcement/investigatory functions.

6. RIPA provides a statutory mechanism for authorising covert surveillance and the use of a "covert human intelligence source" (CHIS) e.g. undercover agents. It also permits access to communications data in specific circumstances.

Types of Surveillance

7. Surveillance may be overt or covert.

8. Most of the surveillance carried out by the Council is done overtly – there is nothing secretive, clandestine or hidden about it. In many cases, officers will be behaving in the same way as a normal member of the public, and/or will be going about Council business openly. Similarly, surveillance will be overt if the subject has been <u>told</u> it will happen (e.g. where a noisy householder is warned that noise will be recorded if it continues).

9. Surveillance is covert only if it is calculated to ensure that persons who are subject to the surveillance are unaware that it is taking place. RIPA regulates two types of covert surveillance.

10. "Directed surveillance" means covert surveillance that is undertaken:

- in connection with a specific investigation or operation
- which is likely to result in the obtaining of private information about a person (whether or not one specifically identified for the purposes of the investigation or operation)

'Private information' is defined in the Act as ~~means~~ information relating to a person's private and family life, their home and their correspondence. However the concept of private information is more broadly defined in the 'Covert Surveillance etc Code of Practice' and the Office of Surveillance Commissioner 'Procedures and Guidance' to include those professional and business activities for which there is a reasonable expectation of privacy.

11. Directed surveillance does not include information gathered by way of an immediate response to events or circumstances the nature of which is such that it would not be reasonably practicable for an authorisation to be sought for the carrying out of the surveillance. Directed surveillance may, in the case of a local Authority, only be carried out for the purposes of "preventing or detecting crime'

12. The fact that covert surveillance occurs in a public place or on business premises does not mean that it cannot result in the obtaining of private information about a person. Prolonged surveillance targeted on a single person will usually result in the obtaining of private information about that person as well as others that he or she comes into contact or associates with.

13 An example of directed surveillance would be when officers follow a person over a period to find out whether they are working at the same time as claiming benefit. Similarly, although town centre CCTV cameras will not normally require authorisation, if a camera is directed in such a way as to observe a particular individual, authorisation may be required.

14. "Intrusive surveillance" means covert surveillance conducted by means of a person or device located inside residential premises or a private vehicle. A local authority cannot carry out intrusive surveillance.

Conduct and Use of Covert Human Intelligence Resource (CHIS)

15. A person is a **CHIS** if he or she establishes a relationship with another person in order to covertly obtain or disclose information. There are special rules relating to the management and use of information supplied by a CHIS and a duty of care is owed to the informant in how the information is used.

The conduct or use of a CHIS requires prior authorisation. Again, a CHIS may only be used for the purposes of "preventing or detecting crime or of preventing disorder."

16. RIPA ~~does~~ may not apply in circumstances where members of the public volunteer information to the Council as part of their normal civic ~~responsibilities~~responsibilities; however this will depend on how the information has been obtained. If the informant has obtained it as an 'insider' i.e. in the course of a personal or other relationship or '*as a result of the existence of such a relationship'* then the informant is likely to be a CHIS even if the relationship was not formed or maintained for that purpose.

If the informant has obtained the information as an outside observer then he is not a CHIS.

~~or w~~Where contact numbers are set up to receive information then it is unlikely that the informant will be a CHIS and ~~. S~~similarly, people who complain about anti- social behaviour, and are asked to keep a diary, will not normally be a CHIS because they are not being required to establish or maintain a relationship for a covert purpose.
~~social behaviour, and are asked to keep a diary, will not normally be a CHIS because they are not being required to establish or maintain a relationship for a covert purpose.~~

~~16. The conduct or use of a CHIS requires prior authorisation. Again, a CHIS may only be used for the purposes of "preventing or detecting crime or of preventing disorder."~~

Communications Data

17. This is data held by telecommunications companies and internet service providers. Examples of communications data that may be acquired with authorisation for a specified operation include:

- names
- addresses
- telephone numbers
- IP addresses – when a session online started and ended and when an email server was accessed but not the website addresses viewed
- geographical location of the calling or the called parties.

18. Communications data does not monitor content. The sole grounds for taking action under these provisions is for the purposes of "preventing or detecting crime'

Online Covert Activity

19. The use of the internet may be required to gather information during an operation, which may amount to directed surveillance. The Home Office advises that where there is an intention to use the internet as part of an investigation and private information is likely to be obtained, consideration should be given for the need of an authorisation and that:

- Officers must not create a false identity in order to 'befriend' individuals on social networks without an authorisation under RIPA.
- officers viewing an individual's public profile on a social network should do so only to the minimum degree necessary and proportionate in order to obtain evidence to support or refute the suspicions or allegations under investigation
- repeated viewing of open profiles on social networks to gather evidence or to monitor an individual's status, must only take place once RIPA authorisation has been granted and approved by a Magistrate
- Officers should be aware that it may not be possible to verify the accuracy of information on social networks and, if such information is to be used as evidence, take reasonable steps to ensure its validity.

Further, where an investigator may need to communicate covertly online, for example, contacting individuals using social media websites, a CHIS authorisation should be considered.

Authorisation Process

20. From 1 November 2012 a local authority who wishes to authorise the use of directed surveillance, the collection of communications data or the use of a CHIS will need to obtain an order approving the required action from the Magistrates Court before that action can take effect.

20. The new judicial approval is in addition to the Council's own internal authorisation conducted under the RIPA Codes of Practice.

21. Also from the 1 November 2012 local authorities will only be able to obtain RIPA authorisation when investigating particular types of criminal offences.

    - Those which attract a maximum custodial sentence of six months or more
    - Those offences relating to the underage sale of alcohol or tobacco

Internal Process

21. Requests to undertake directed surveillance, or to use a CHIS or to collect communications data can only be lawfully carried out if properly authorised and in strict accordance with the terms of the authorisation.

22. The Secretary of State specifies by statutory instrument the level of officer who may act as Authorising Officers. In this Council, the Chief Executive and the Directors, under the Constitution (Part 3, Sec 7 (3) (iii)) are designated to act as Authorising Officers. The Chief Executive or Monitoring Officer may designate other officers to act as Authorising Officers. Authorisations must not be allowed to lapse. They must be reviewed regularly or cancelled.

23. The steps to be followed for each procedure are shown in the flow charts in Appendix 1.

24. For Directed Surveillance or the use of a CHIS or Communications data, only the approved RIPA forms, available on the Home Office website: (http://www.homeoffice.gov.uk/counter-terrorism/regulation-investigatory-powers/ripa-forms/) may be used. Any other form will be rejected by the Authorising Officer. An applicant officer, or an Authorising Officer, if in doubt about the process to be followed, should always seek the advice of the Head of Legal and Support Services or the Senior Auditor before applying for, or issuing, an authorisation under RIPA.

25. The officer requesting the authorisation will be responsible for ensuring that copies of all forms are forwarded to the Senior Auditor within seven days of issue. As a control measure the Senior Auditor will supply the applicant officer with a referenced copy of the authorisation which they should keep in their department in secure storage. Officers should ensure that material

passing between them is sent in such a way that it cannot be read or intercepted by other people.

26. A copy of the form should also be forwarded to the Council's Legal Services Team who will commence proceedings for appearance at the Magistrates Court to seek final judicial approval.

Considering an Application for Authorisation

27. Before signing a form, the Authorising Officer must have regard to this Policy and Procedure, to any relevant Code of Practice, to any advice from the Head of Legal and Support Services or Senior Auditor and to any other relevant guidance.

28. The Authorising Officer must also satisfy himself/herself that the RIPA authorisation is:

- **in accordance with the law**;
- **necessary** in the circumstances of the particular case on the ground of preventing or detecting crime or preventing disorder; and
- **proportionate** to what it seeks to achieve.

29. In considering whether or not the proposed surveillance is proportionate, the Authorising Officer will need to consider whether there are other more non-intrusive ways of achieving the desired outcome. If there are none, the Authorising Officer will need to consider whether the proposed surveillance is no more than necessary to achieve the objective as the least intrusive method will be considered proportionate by the courts.

30. The Authorising Officer will also need to take into account the risk of intrusion into the privacy of persons other than the specified subject of the surveillance. This is known as collateral intrusion. Measures must be taken whenever practicable to avoid or minimise, so far as practicable, collateral intrusion.

31. When authorising the conduct or use of a CHIS the Authorising Officer must also be satisfied that appropriate arrangements are in place for the management and oversight of the CHIS. This must address health and safety issues through a risk assessment. He or she must also have regard to any adverse impact on community confidence that may result from the use or conduct of the information obtained.

Judicial Approval

32. Once the Authorising Officer is satisfied that the RIPA is necessary they will instruct Legal Services to seek approval from the Magistrates Court.

33. Legal Services will request a hearing date from the Courts and which will need to be taken into account when considering any scheduled timetable connected to the matter being investigated.

34. At the hearing the Council will provide the Court with a copy of the authorisation signed by the Authorising Officer together with any supporting documents relevant to the matter showing the necessity of the authorisation and which contains all the information relied upon. Also included will be a summary of the circumstances of the case.

35. The hearing will be in private heard by a single Magistrate/District Judge who will read and consider the application. They may ask questions of the authority in order to satisfy themselves of the necessity and reasonableness of the request.

36. On reviewing the papers and hearing the application the Court will determine whether they are satisfied that there are reasonable grounds for believing that the authorisation is necessary and proportionate. In addition they must be satisfied that the Authorising Officer had the relevant authority to authorise the Council's own internal authorisation prior to it passing to the Court.

37. In considering the application the Court may decide to

- **Approve the Grant or renewal of an authorisation or notice**
  The grant or renewal of the RIPA authorisation or notice will then take effect and the local authority may proceed to use surveillance in that particular case.

  In relation to Communications Data, the Council will be responsible for providing a copy of the order to the SPoC.

- **Refuse to approve the grant or renewal of an authorisation or notice**
  The RIPA authorisation or notice will not take effect and the Council may **not** use surveillance in that case.

  Where an application has been refused the Council may wish to consider the reasons for that refusal. For example, a technical error in the form may be remedied without the need to go through the internal authorisation process again. The local authority may then wish to reapply for judicial approval once those steps have been taken.

- **Refuse to approve the grant or renewal and quash the authorisation or notice**
  This applies where a magistrates' court refuses to approve the grant, giving or renewal of an authorisation or notice and decides to quash the original authorisation or notice.
  The court must not exercise its power to quash that authorisation or notice unless the applicant has had at least 2 business days from the date of the refusal in which to make representations.

Urgent Judicial Approval of Applications

38. Urgent approvals should not be necessary.

    If the approval is urgent and cannot be handled the next working day then you should:

    i) Phone the Court's out of hours legal staff contact. You will be asked about the basic facts and urgency of the authorisation. If the police are involved in the investigation you will need to address why they cannot make a RIPA authorisation

ii) If urgency is agreed, then arrangements will be made for a suitable Magistrate to consider the application. You will be told where to attend and give evidence.

iii) Attend the hearing as directed with two copies of both the counter-signed RIPA authorisation form or notice and the accompanying judicial application/order form.

Central Co-ordination

39. The Chief Executive will be the Senior Responsible Officer for the overall implementation of RIPA. The Head of Legal and Support Services will be responsible for:
    - giving advice and assistance to all staff concerned with the operation of the Act;
    - arranging training for all staff concerned with the operation of the Act;
    - maintaining and keeping up to date this corporate policy and procedure.
    - The Senior Auditor will be responsible for:
    - maintaining a central and up to date record of all authorisations;
    - along with the Head of Legal and Support Services, giving advice and assistance to all staff concerned with the operation of the Act;
    - allocating reference numbers to authorisations;

Working with other Agencies

40. When some other agency has been instructed on behalf of the Council to undertake any action under RIPA, this Policy and Procedure must be used and the agency given explicit instructions on what it may do and how it may do it.

41. When some other agency (e.g. Police, Customs & Revenue etc.):

    - wish to use the Council's resources (e.g. CCTV surveillance systems) for RIPA purposes, that agency must use its own RIPA procedures and, before any officer agrees to allow the Council's resources to be used for the other agency's purposes he or she must obtain a copy of that agency's RIPA form for the record (a copy of which must be passed to the Senior Auditor for inclusion on the central register);
    - wish to use the Council's premises for their own RIPA action, and is expressly seeking assistance from the Council, the officer should normally grant the request unless there are security or other good operational or managerial reasons as to why the Council's premises should not be used for the agency's activities. Suitable insurance or other appropriate indemnities may need to be sought. In such cases, the Council's own RIPA forms should not be used as the Council is only assisting and not involved in the RIPA activity of the external agency.

Other Sources of Information

42. The Home Office has issued Codes of Practice on surveillance, CHIS and the collection of communications data. These Codes of Practice supplement this policy and procedure document and should be used as a binding source of

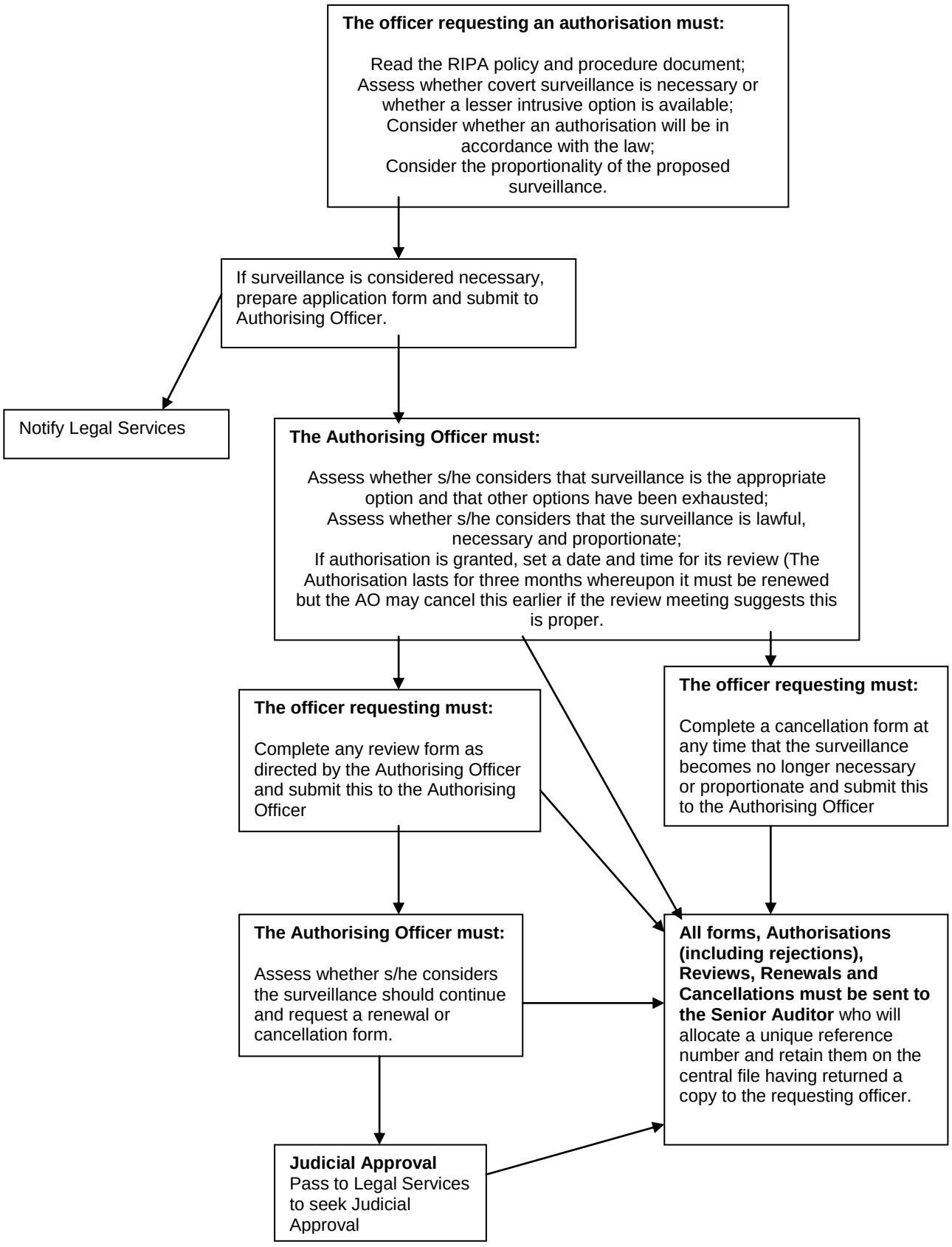
reference by all those officers whose task it is to apply the provisions of RIPA and its subordinate legislation.

ASG Revised Dec 2006
ASG Reviewed May 2009
AW Reviewed and updated June 2010
ASG Revised March 2012
HO Guidance issued October 2012
RH Reviewed and updated September 2013
DMG Reviewed and updated October 2015
Approved by Audit and Governance Committee 9 December 2015
Approved by Council 12 January 2016

Appendix 1

RIPA – DIRECTED SURVEILLANCE / USE OF CHIS PROCEDURE

(Note: Only the Chief Executive may authorise the use of a juvenile or vulnerable individual as a CHIS)



RIPA – COMMUNICATIONS DATA PROCEDURE