APPENDIX 1

CHESHIRE EAST COUNCIL

SURVEILLANCE UNDER THE REGULATION OF INVESTIGATORY POWERS ACT 2000 (RIPA)

POLICY AND PROCEDURE

Applications for Authorisation to carry out Surveillance and for the use of Covert Human Intelligence Sources

This document sets out the requirements for gaining authorisation under RIPA, the persons able to grant authorisation, circumstances when authorisation will be required and the storage and maintenance of records of authorisation

SURVEILLANCE UNDER THE REGULATION OF INVESTIGATORY POWERS ACT 2000 (RIPA)

POLICY

P1 BACKGROUND

P1.1 The Regulation of Investigatory Powers Act 2000 (RIPA) came into effect in September 2000. It establishes a regulatory framework for the use of covert surveillance by setting up an authorisation procedure. Covert surveillance is defined in Section 26(9) (a) of RIPA as "*any 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*". RIPA seeks to ensure that public authorities only use covert surveillance where it is necessary for a specific, legally prescribed purpose, and that the surveillance is carried out in such a way that the risk of infringing the rights of individuals is kept to an absolute minimum.

P1.2 Some surveillance operations may interfere with Article 8 of the Human Rights Act 1998 which provides that everyone has the right to respect for his private and family life, his home and correspondence. This right is subject to an important qualification - Paragraph 2 of Article 8 provides that:

"There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others."

P1.3 RIPA therefore protects an individual's rights and freedoms that are guaranteed by the European Convention and given further effect by the Human Rights Act 1998, whilst allowing a public authority to carry out certain, necessary covert surveillance.

P2 INTRODUCTION

P2.1 Cheshire East Council will, on occasion, need to use covert surveillance in order to carry out its enforcement functions effectively. Examples of enforcement activities which may require the use of RIPA include benefit fraud, planning enforcement, licensing enforcement, trading standards, environmental health, community safety investigations and breaches of tenancy conditions related to anti-social behaviour and crime. **A local authority may only use covert surveillance for the purpose of the prevention or detection of crime or the prevention of disorder.**

P2.2 Surveillance by a public authority is likely to constitute an infringement of an individual's rights and freedoms which are protected by the Human Rights Act 1998. However, by following the authorisation procedures set out by RIPA, officers of the Council are ensuring that they can demonstrate that the surveillance is necessary for a purpose permitted by the Human Rights Act 1998 and that it is a proportionate measure to take, given all the circumstances. Compliance with RIPA will significantly reduce the likelihood of any surveillance carried out by the Council being unlawful and therefore subject to legal challenge.

P3 CHESHIRE EAST COUNCIL'S POLICY IN ACCORDANCE WITH RIPA AND THE HOME OFFICE CODES OF PRACTICE

P3.1 The purpose of this policy and its associated procedure is to reinforce the requirements of RIPA and its Codes of Practice, to ensure compliance with RIPA, to protect the rights of individuals and to minimise the risk of legal challenge as a result of officer actions.

P3.2 The Council is fully committed to complying with the Human Rights Act 1998 and RIPA. In order to ensure compliance, all directed covert surveillance must be carried out in accordance with the legislative framework and the Council's RIPA policy and procedure.

P3.3 In addition to all legislative, policy and procedural requirements, officers must have regard to the Statutory Codes of Practice on the use of covert surveillance and the use of a covert human intelligence source ("CHIS"), issued by the Home Office. Officers must also have regard to any other guidelines that may be published from time to time.

P3.4 In particular, any legislative restrictions on the type of covert surveillance that a local authority is authorised to carry out must be observed; all covert surveillance must be properly authorised and recorded; the tests of necessity and proportionality must be satisfied; and the potential for collateral intrusion must be considered and minimised. Definitions of terms are included in the RIPA procedure.

P3.5 Any officer intending to undertake covert surveillance or use a covert human intelligence source will only do so if the evidence or intelligence sought cannot be obtained by other means.

P3.6 Embarking upon covert surveillance or the use of a covert human intelligence source without authorisation or conducting covert surveillance outside the scope of the authorisation will not only mean that the "protective umbrella" of RIPA is unavailable but may result in disciplinary action being taken against the officer/officers involved. RIPA has also established an Independent Tribunal which has full powers to investigate and decide any case within its jurisdiction.

P3.7 The Council's RIPA policy and procedure will be reviewed annually, or sooner if necessary (e.g. in the event of legislation being amended or revoked).

P4 APPLICATION

P4.1 The Council's policy is operational forthwith and applies to all Council staff employed under a permanent, temporary, fixed term or casual contract. It also applies to any contractors and/or subcontractors employed by the Council to undertake activities covered by this policy and procedure. All relevant Council contracts issued to contractors/subcontractors will include a term that this policy and associated procedures are to be observed when operating on behalf of the Council.

P4.2 A copy of this policy document together with the Home Office Codes of Practice and Investigatory Powers Tribunal leaflets will be made available for public inspection at the Council offices' Reception Areas and on the Council's website.

SURVEILLANCE UNDER THE REGULATION OF INVESTIGATORY POWERS ACT 2000 (RIPA)

PROCEDURE

1 TYPES OF SURVEILLANCE

1.1 There are three types of covert surveillance: "intrusive surveillance", "directed surveillance" and surveillance by means of a "covert human intelligence source" (a "CHIS").

1.2 Local authorities are **not** authorised to carry out any form of intrusive surveillance.

1.2.1 Intrusive surveillance is defined in section 26(3) of RIPA as covert surveillance that:

- is carried out in relation to anything taking place on any residential premises or in any private vehicle; and
- involves the presence of an individual on the premises or in the vehicle or is carried out by means of a surveillance device (e.g. a listening device in a person's home or in their private vehicle).

1.3 Local authorities are permitted to carry out directed surveillance.

1.3.1 Directed surveillance is defined in Section 26(2) of RIPA as surveillance which is covert, but not intrusive, and undertaken:

- for the purposes of a specific investigation or specific operation;
- in such a manner as it is likely to result in the obtaining of **private information** (see Section 13) about the person (whether or not one specifically identified for the purposes of the investigation or operation); and
- otherwise than by way of an immediate response to events or circumstances, the nature of which is such that it would not be reasonably practical for an authorisation under Part II of RIPA to be sought for the carrying out of the surveillance.

1.3.2 Directed surveillance will only be carried out on residential premises if a member of the public has requested help or made a complaint to the Council and written permission to conduct the surveillance has been obtained from the householder or tenant from whose premises the surveillance will be carried out. See also paragraph 5.7.

1.3.3 Closed Circuit Television (CCTV) systems are normally not within the scope of RIPA. However, if they are used for a specific operation or investigation, or if automatic facial recognition by means of CCTV is used, authorisation for the use of directed surveillance must be obtained in accordance with this procedure.

1.3.4 A protocol has been agreed with the police regarding the use of CCTV to assist with their investigations. Where the police wish to use the council's CCTV facilities it is essential that a copy of the police's authorised RIPA application is viewed by the CCTV Manager.

1.4 Local authorities are permitted to use a covert human intelligence source.

1.4.1 A covert human intelligence source (a "CHIS") is defined by section 26(8) of RIPA as a person who:

- establishes or maintains a personal or other relationship with another person for the covert purpose of facilitating the doing of anything falling within the following two paragraphs;

- covertly uses such a relationship to obtain information or to provide access to any information to another person: or

- covertly discloses information obtained by the use of such a relationship or as a consequence of the existence of such a relationship.

1.5 The provisions of RIPA are not intended to apply to circumstances where members of the public volunteer information as part of their civic duties or to contact numbers set up to receive information.

1.6 An authorisation under Part II of RIPA will provide lawful authority for the use of a covert human intelligence source ("CHIS"). Use of a source without an authorisation will not be unlawful but where there is interference by a public authority with the right to respect for private and family life guaranteed under Article 8 of the Human Rights Act 1998 and there is no other lawful authority the consequences of not obtaining an authorisation under RIPA may be that the action is unlawful by virtue of the Human Rights Act 1998.

1.7 Where the use or conduct of a CHIS is likely to interfere with an individual's Article 8 rights an authorisation must be sought in order to ensure that the action is carried out in accordance with the law.

2 OFFICERS ABLE TO MAKE AUTHORISATIONS

2.1 Under Section 28(3) of RIPA an authorisation for directed surveillance or the use of a covert human intelligence source ("CHIS") may be granted by an Authorising Officer where he believes that the authorisation is

Necessary in the circumstances of the particular case:

- for the purpose of preventing or detecting crime or of preventing disorder;

and,

Proportionate to what it seeks to achieve.

2.2 Detecting crime includes establishing by whom, for what purpose, by what means and generally in what circumstances any crime was committed, the gathering of

evidence for use in any legal proceedings and the apprehension of the person (or persons) by whom any crime was committed.

2.3 The Home Office recently published three new orders under Part 2 of the Regulation of Investigatory Powers Act 2000 which came into force on 6th April 2010. Under the Regulation of Investigatory Powers(Directed Surveillance and Covert Human Intelligence Sources Order 2010 (2010/521) the Authorising Officers for Local Authorities are restricted to Director, Head of Service, Service Manager or equivalent. In Cheshire East Council the Authorising Officers are the Chief Executive and members of the Corporate Management Team.

In cases in which confidential information is likely to be obtained or in which Section 15.2 or 15.3 of this procedure applies.:

- The Chief Executive, or (in her absence)
- A Director

2.4 Authorising Officers should not be responsible for authorising investigations or operations in which they have had or are likely to have any direct involvement. When such authorisation is required, this will be sought from an alternative authorising officer, as appropriate. When such an investigation or operation has to be authorised in this way, the Central Record of Authorisations should highlight this and the attention of the National Surveillance Commissioner or Inspector should be drawn to it during his next inspection.

2.5 Under the revised Code of Practice it is considered good practice for every public authority to appoint a Senior Responsible Officer (SRO). Within Cheshire East Council this is the Borough Solicitor, who is responsible for:

- the integrity of the process in place within the public authority for the management of CHIS and Directed Surveillance;
- compliance with Part 2 of the Act and with the Codes;
- engagement with the OSC inspectors when they conduct their inspections, where applicable; and
- where necessary, oversight of the implementation of post-inspection action plans approved by the relevant oversight Commissioner.

In addition under the new code councillors have been given a formal scrutiny role in relation to RIPA. The new code states that, at least once a year, they should review the authority's use of RIPA and set the general surveillance policy. They should also consider internal reports on the use of RIPA at least on a quarterly basis to ensure that it is being used consistently as per the council's policy and that the policy remains fit for purpose. It is however emphasised that councillors should not be involved in making decisions on specific authorisations.

3 THE TESTS OF NECESSITY AND PROPORTIONALITY

3.1 Directed covert surveillance or the use of a covert human intelligence source ("CHIS") should only be authorised if the Authorising Officer is satisfied that:

- **The action is NECESSARY (in a democratic society) on the following grounds:**

- For the prevention or detection of crime or the prevention of disorder

and,

- **The surveillance is PROPORTIONATE - The Human Rights Act defines a measure or action as proportionate if it:**

  - Impairs as little as possible the rights and freedoms (of the individual concerned and of innocent third parties),
  - Is carefully designed to meet the objectives in question, is not arbitrary, unfair, or based on irrational considerations.

4 COLLATERAL INTRUSION

4.1 In the case of both directed covert surveillance and the use of a covert human intelligence source, the Authorising Officer must also take into account the risk of intrusion into the privacy of persons other than those who are directly the subject of the investigation or operation. This is termed "collateral intrusion".

4.2 Officers carrying out the surveillance should inform the Authorising Officer if the investigation or operation unexpectedly interferes with the privacy of individuals who are not covered by the authorisation. Consideration should be given to whether the authorisation should be amended and re-authorised or whether a new authorisation is required.

4.3 Any officer applying for or granting an authorisation will need to be aware of the particular sensitivities in the local community where the surveillance is taking place and of similar activities being undertaken by other public authorities which could impact on the deployment of surveillance.

5 APPLICATIONS FOR AUTHORISATION TO CARRY OUT DIRECTED SURVEILLANCE OR USE A COVERT HUMAN INTELLIGENCE SOURCE ("CHIS")

5.1 An application for authorisation must be in writing and on the appropriate form which must be completed in full.

5.2 Officers should ensure that they use the current form obtained from the Home Office website (http://security.homeoffice.gov.uk/ripa/)

5.3 Before applications are authorised, they must be forwarded to the Compliance Unit, Internal Audit, to be checked and recorded in the Central Register of Authorisations (Section 12).

5.4 Officers requesting authorisation for directed surveillance should consider whether it is necessary to complete a risk assessment, which should be submitted with the authorisation request, where applicable. Officers requesting authorisation to use a covert human intelligence source ("CHIS") must always complete a risk assessment and submit it with the authorisation request (see also Section 15).

5.5 All relevant documentation, including a copy of the authorisation, a record of the period over which surveillance has taken place, any risk assessment, notebooks, surveillance logs and other ancillary documentation will be retained at departmental level for a period of six years from the date of commencement of surveillance, at which point they will be securely destroyed.

5.6 Other than in exceptional circumstances, the investigation of noise complaints will only be carried out by means of **overt surveillance.** Therefore, an authorisation will **not** normally be required to install a noise recording or monitoring device in a property neighbouring premises that are subject to a noise level complaint, provided the following is observed: (i) the written permission of the complainant must be obtained, (ii) the occupant of the monitored premises must receive notice in writing that noise recording/monitoring equipment may be installed in a neighbouring property (thus rendering the surveillance overt), and (iii) the surveillance must be carried out within a period of three calendar months from the date of the notice. At the end of the three month period, the surveillance must cease or, if surveillance is to continue, either a further notice must be served on the occupant of the monitored premises or an authorisation to conduct (covert) directed surveillance will be required.

6 URGENT AUTHORISATIONS

6.1 In urgent cases authorisation may be given orally by the Authorising Officer. In these cases, a statement that the Authorising Officer has expressly authorised the activity should be recorded in writing within 72 hours and the appropriate section of the application form should also be completed and forwarded to the Compliance Unit immediately.

6.2 A case would not normally be regarded as urgent unless the time that would elapse before the Authorising Officer was available to grant the written authorisation would, in the judgment of the person giving the authorisation, be likely to endanger life or jeopardise the investigation or operation for which the authorisation was being given. An authorisation is not to be regarded as urgent where the need for an authorisation has been neglected or overlooked or if the urgency is of the Authorising Officers own making.

6.3 Authorising Officers should not be responsible for authorising investigations or operations in which they are directly involved. However, if, in exceptional circumstances, this is unavoidable, the central Record of Authorisations should highlight this and the attention of the Commissioner or Inspector should be drawn to it during the next inspection.

6.4 In urgent cases, in addition to the information to be provided in an application for authorisation, the reasons why the Authorising Officer considered the case so urgent that an oral instead of a written authorisation was given should be recorded.

6.5 Only the Authorising Officers listed in paragraph 2.3 above may authorise applications, including in urgent cases.

7 DURATION OF AUTHORISATIONS

7.1 A written authorisation granted by an Authorising Officer will cease to have effect (unless renewed) either on specific cancellation or at the end of a period of three months (directed surveillance) or twelve months ("CHIS"), beginning with the day on which it took effect.

7.2 Urgent authorisations will, unless renewed, cease to have effect after 72 hours, beginning with the time when the authorisation was granted or renewed.

8 REVIEWS

8.1 Regular reviews of authorisations by the Authorising Officer should be undertaken to assess the need for surveillance to continue. All reviews should be completed using the appropriate form.

8.2 Officers should ensure that they use the current form obtained from the Home Office website (http://security.homeoffice.gov.uk/ripa/)

8.3 Particular attention is drawn to the need to review authorisations frequently where surveillance provides access to confidential information or involves collateral intrusion.

8.4 Review documentation, including the frequency of reviews and a record of the result of each review, will be retained for a period of six years, at which point it will be destroyed. Documentation detailing any instruction given by the Authorising Officer will be retained for a period of six years at departmental level, at which point it will be securely destroyed.

9 RENEWALS

9.1 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, he may renew it in writing. Renewals may also be granted orally in urgent cases and last for a period of 72 hours.

9.2 All applications for the Renewal of an Authorisation for Directed Surveillance should be on the appropriate form which must be completed in full.

9.3 Officers should ensure that they use the current form obtained from the Home Office website (http://security.homeoffice.gov.uk/ripa/)

9.4 Any renewal documentation, together with any supporting documentation, and any documentation detailing any instruction issued by the Authorising Officer will be retained for a period of six years at departmental level, at which point it will be securely destroyed.

9.5 Copies of all renewals should be sent (securely transmitted) to the Compliance Unit.

10 CANCELLATIONS AND HANDLING OF SURVEILLANCE PRODUCT

10.1 The Authorising Officer who granted or last renewed the authorisations must cancel it if he is satisfied that the activity no longer meets the criteria upon which it was authorised or it has fulfilled its objective. If the Authorising Officer is no longer available, this duty will fall on the person who has taken over the role of the Authorising Officer.

10.2 Officers should ensure that they use the current form obtained from the Home Office website (http://security.homeoffice.gov.uk/ripa/).

10.3 On cancellation of an authorisation, the Authorising Officer must be satisfied that the product of any surveillance is properly retained and stored or destroyed. If the surveillance product is of no evidential or intelligence value, it should be destroyed without delay in accordance with Data Protection requirements. If the surveillance product is of potential evidential or intelligence value, it should be retained on the legal file in accordance with established disclosure requirements, commensurate to any subsequent review.

11 CESSATION OF ACTIVITY

11.1 As soon as the decision is taken that the authorised activity should be discontinued, the instruction must be given to those involved to stop all surveillance of the subject or to cease using the covert human intelligence source.

11.2 Documentation detailing the date and time when any cancellation instruction was given by the Authorising Officer will be retained for a period of six years, at which point it will be securely destroyed.

12 CENTRAL RECORD OF AUTHORISATIONS

12.1 A Central Record of Authorisations will be held and updated whenever an authorisation is granted, renewed or cancelled. The Compliance Unit is responsible for ensuring that a Central Record is maintained. The record will be made available to the relevant Commissioner or an Inspector from the Office of Surveillance Commissioners, upon request. These records should be retained for a period of three years from the ending of the authorisation, at which point they will be securely destroyed.

12.2 In respect of directed surveillance the Central Record of Authorisations will contain a copy of the authorisation together with the following information:

- the type of authorisation: the date the authorisation was given;
- name of the authorising officer;
- the departmental reference number of the investigation or operation
- the title of the investigation or operation, including a brief description and names of subjects, if known;

- whether the urgency provisions were used, and if so why;
- in the case of a self authorisation by the Authorising Officer, a statement in writing that he/she expressly authorised the action (only in exceptional circumstances)
- if the authorisation is renewed, when it was renewed and who authorised the renewal, including the name and grade of the authorising officer;
- whether the investigation or operation is likely to result in obtaining confidential information;
- the date the authorisation was cancelled.
- a copy of the Privacy Impact Assessment

12.3 In respect of a covert human intelligence source ("CHIS") the Central Record of Authorisations will contain the following additional information:

- a copy of the authorisation together with any supplementary documentation and notification of the approval given by the Authorising Officer;
- a copy of any renewal of an authorisation together with the supporting documentation submitted when the renewal was requested;
- the reason why the person renewing an authorisation considered it necessary to do so;
- any urgent authorisation which was granted or renewed orally (in an urgent case) and the reason why the case was considered urgent;
- the risk assessment made in relation to the source ("CHIS");
- a record of the results of any reviews of the authorisation;
- the reasons, if any, for not renewing an authorisation;
- the reasons for cancelling an authorisation - cancellations are to be completed on the appropriate form
- the date and time when any instruction was given by the Authorising Officer to cease using a "CHIS".
- The Privacy Impact Assessment

13 PRIVATE INFORMATION

13.1 "Private information" is defined in Section 26(10) of RIPA as including any information relating to a person's private or family life. The concept of private information should be broadly interpreted to include an individual's private or

personal relationship with others and should also be taken to include activities of a professional or business nature. Family life should be treated as extending beyond the formal relationships created by marriage.

14 CONFIDENTIAL INFORMATION

14.1 The Act does not provide any special protection for confidential information. Nevertheless, particular care should be taken in cases where the subject of the investigation might expect a high degree of privacy or where confidential information is involved. Confidential information consists of matters subject to legal privilege, confidential personal information or confidential journalistic material.

14.2 In cases where, through the use of surveillance, it is likely that knowledge of confidential information will be acquired, the use of surveillance is subject to a higher level of authorisation. In cases where confidential information is likely to be acquired it will be the Chief Executive or (in his/her absence) a Director, who must give the authorisation. The Act does not provide any special protection for legally privileged information. Nevertheless, such information is particularly sensitive, and surveillance which acquires such material may engage Article 6 and Article 8 of the European Convention/Human Rights Act 1998.

14.3 An application for surveillance which is likely to result in the acquisition of legally privileged information should only be made in exceptional and compelling circumstances. The application should include, in addition to the reasons why it is considered necessary for the surveillance to take place, an assessment of how likely it is that the information subject to legal privilege will be acquired. In addition the application will clearly state whether the purpose (or one of the purposes) of the surveillance is to obtain legally privileged information. Full regard should be had to the particular proportionality issues such surveillance raises.

14.4 Similar considerations must be given to authorisations that involve confidential personal information and journalistic material. In cases where confidential personal information and confidential journalistic material has been acquired and retained, the matter should be reported to the relevant Commissioner or Inspector during his next inspection and the material be made available to him if requested.

15 ADDITIONAL REQUIREMENTS FOR AUTHORISATION OF COVERT HUMAN INTELLIGENCE SOURCES ONLY

15.1 Covert human intelligence sources may only be authorised if the following additional arrangements are in place:

- There is an employee of the Council with day to day responsibility for dealing with the source and for the source's security and welfare.

- There is a Senior Officer who has general oversight of the use made of the source.

- An officer will be responsible for maintaining a record of the use made of the source.

- Those records will contain any matters specified by the Secretary of State – The Regulation of Investigatory Powers (Source Records) Regulations 2000 (SI 2000/2725) set out these matters.

- That records disclosing the identity of the source and the information provided by him/her will not be made available to others except on a need to know basis.

15.2 Vulnerable individuals (a person who is in need of community care services by reason of mental or other disability, age or illness and who is or may be unable to take care or protect himself against significant harm or exploitation) may be authorised to act as a CHIS **only in the most exceptional circumstances.** Authorisation must be given by the Chief Executive or (in his/her absence) the Borough Solicitor.

15.3 Authorisations for juvenile sources (under 18) should only be granted if the provisions contained in The Regulation of Investigatory Powers (Juveniles) Order 2000 (SI 2000/2793) are satisfied. Any authorisation should be granted by the Chief Executive or (in his/her absence) a Director. The duration of an authorisation for the use or conduct of juvenile sources is **one month. A source under the age of 16 must not be authorised to give information against his parents or any person who has parental responsibility for him.**

15.4 If a juvenile source (under 18) is to be used, the authorising officer is responsible for obtaining the written consent of the parent or guardian or the person caring for the juvenile, unless to do so would compromise the juvenile's welfare or safety. The authorising officer is also responsible for ensuring that an appropriate adult is present at any meeting. An appropriate adult means a parent or guardian, person who has assumed responsibility for the wellbeing of the CHIS or, in their absence, a person who is responsible for the wellbeing of the CHIS and who is over 18 who is neither a member of, nor employed by, the Council.

15.5 **On no occasion should the use or conduct of a source under 16 years of age be authorised to give information against his parent or any person who has parental responsibility for him/her.**

15.6 The processing of information obtained as a result of surveillance will be restricted to specified employees employed in Internal Audit. Only relevant senior managers will have access to the information collected to enable appropriate action to be taken. They will respect the confidentiality of all information and only disclose the information to other appropriate senior managers where further action is required.

15.7 When a covert human intelligence source ("CHIS") is used, a "Handler" (who can be an officer of the Council), and who must have received appropriate training, should be designated as having the day to day responsibility for dealing with the "CHIS". This responsibility shall extend to security, safety and welfare of the "CHIS". In addition, a "Controller" should be designated to have the general oversight of the use made of the "CHIS". These requirements also apply in cases in which the "CHIS" is an officer of the Council.

15.8 The officer requesting authorisation for the use of a covert human intelligence source ("CHIS") must also complete a risk assessment and submit it to the Authorising Officer together with the authorisation request.

16 MONITORING OF RECORDS

16.1 The Borough Solicitor to the Council will be responsible for monitoring authorisations and conducting a quarterly review of applications, authorisations, refusals, reviews renewals and cancellations.

17 SCRUTINY

17.1.1 The Borough Solicitor will ensure that an annual report is submitted to the Council's Audit & Governance Committee. The report will include details of the overall number and type of authorisations granted and the outcome of the case, where known. In addition, the report will provide a breakdown of the same information by service or groups of services, as appropriate.

17.2 The report should also include the results of the most recent inspection carried out by a representative of the Office of Surveillance Commissioners, where applicable (inspections may not take place annually).

18 FURTHER INFORMATION

18.1 For further guidance please see the relevant Home Office guidance available from the Home Office website http://www.homeoffice.gov.uk/ or contact Legal Services.