Hastings Borough Council

Regulation of Investigatory Powers Act 2000

(RIPA)

Corporate Policy and Procedures

and

Codes of Practice and Guidance

This policy was adopted by Hastings Borough Council at its Cabinet Meeting on 24 November 2003
Reviewed (April.2006)
Reviewed (March 2009)
Reviewed (June 2011)
Reviewed (December 2012)
Reviewed (June 2018)

Hastings Borough Council, RIPA Corporate Policy and Procedures and Code of Practice
Contents

NB: The Regulation of Investigatory Powers Act 2000 (RIPA) refers to ‘Designated Officers’. For ease of understanding and application within Hastings Borough Council this policy refers to ‘Authorising Officers’.

Furthermore, such officers can only act under RIPA if they have been duly authorised by the Chief Legal Officer and the Corporate Director of Operational Services. The list of Authorised Officers can be found at Appendix 1.

A. Introduction

1. This Corporate Policy and Procedures Document is based upon the requirements of The Regulation of Investigatory Powers Act 2000 (RIPA)(as amended) the Regulation of Investigatory Powers (Directed Surveillance and Covert Human Intelligence Sources) Order 2012 and the Home Office's Code of Practices on Covert Surveillance, and the Covert Human Intelligence Sources (CHIS). It also refers to the Home Office guidance to local authorities on the judicial approval process for RIPA. Covert Surveillance should be used only rarely and in exceptional circumstances. These Codes are to be found at Appendix 7 and Appendix 8 of this policy. The Codes and guidance are also available on the Home Office's website at www.homeoffice.gov.uk. The website Codes should be consulted, from time to time, to ensure that this document remains up to date.

2. The authoritative position on RIPA is the Act itself. Any officer who is unsure about any aspect of this document should, if unsure, contact at the earliest possible opportunity the Council's Legal Services for advice and assistance. Most Council enforcement officers, authorised officers and senior managers have received RIPA training (where appropriate). Any further training will be arranged by Personnel and Organisational Development as and when required. If you need training please request this from your immediate line manager. Copies of this policy and related forms will be placed on the Council's website and on the intranet.

3. The Chief Legal Officer will maintain and check the Corporate Central Register of all RIPA Authorisations, Reviews, Renewals, Cancellations and Rejections. For administration and operational effectiveness the Chief Legal Officer and the Corporate Director of Operational Services are authorised to add or substitute officers authorised for the purposes of RIPA.

4. This policy document is important for the effective and efficient operation of the Council's actions with regard to Covert Surveillance and Covert Human Intelligence Sources. This document will be reviewed annually by the Council's Legal Services. Authorising Officers must bring any suggestions for continuous improvement of this document to the attention of the Chief Legal Officer at the earliest opportunity. If any of the Home Office Codes of Practice change, this document will be amended accordingly.

5. In terms of monitoring e-mails and internet usage, it is important to recognise the important interplay and overlaps with the Council's e-mail and internet policies and guidance, the Telecommunications (Lawful Business Practice)(Interception of Communications) Regulations 2000, The Data Protection Act 1998 and its Codes of Practice. Under normal circumstances the Council's e-mail and internet policies should be used as any surveillance is likely to be more relevant under the contract of employment terms as opposed to RIPA. In 2017 the Council refreshed its Social Media Policy. This can be found on the Council's website.

6. At no time should the Council undertake any surveillance that interferes with any private property. Placing tracking devices on a subject's vehicle or person are not authorised for local authorities and must not be used. Again, if anyone has any doubt as to the Council's RIPA powers then they should contact Legal Services for clarification at the earliest opportunity.

7. Historically, three inspections by the Office of the Surveillance Commissioners have previously been undertaken concerning Hastings Borough Council's use of RIPA procedures. Past criticisms from those inspections have resulted in further training of key staff and further reviews of the Council's policy and procedures and forms. The last

two reports, following inspection, have resulted in positive comments on the Council's policies and procedures.

B. General Information on RIPA

8. This Corporate Policy, Procedures and the Forms provided in this policy document are operative with immediate effect. It is essential, therefore, that Chief Officers and Authorising Officers in their Departments take personal responsibility for the effective and efficient operation of this document in their Departments. As part of this review the forms have been revised using the Home Office templates as amended.

9. It will be the responsibility of Authorising Officers to ensure that their relevant members of staff are suitably trained so as to afford common mistakes appearing on forms for RIPA authorisations.

10. Authorising officers will also ensure that staff who report to them follow this Corporate Policy and Procedures document and do not undertake or carry out any form of surveillance without first obtaining the relevant authorisations in compliance with this document.

11. Authorising Officers must also pay particular attention to Health and Safety issues that may be raised by any proposed surveillance activity. Under no circumstances should an Authorising Officer approve any RIPA form unless, and until s/he is satisfied that the health and safety of Council employees/agents are suitably addressed and/or risks minimised, so far as is possible and proportionate to/with the surveillance being proposed. If an Authorising Officer is in any doubt he should obtain prior guidance on the same from Legal Services.

12. Authorising Officers must acquaint themselves with the relevant Codes of Practice and guidance issued by the Home Office regarding RIPA. These are appended at Appendix 7 and Appendix 8. They are also available on the home office website at www.homeoffice.gov.uk. Any failure to comply exposes the Council to unnecessary legal risks and criticism from the Office of Surveillance Commissioners. Forms must be dealt with promptly.

13. Coming across private/confidential information during surveillance must be given prior thought before any applications are authorised, as failure to do so may invalidate the admissibility of any evidence obtained. Furthermore, thought must be given before any forms are signed to the retention and disposal of any material obtained under a RIPA authorisation. Refer to the Council's Document Retention policy on the website. Where there is any possibility of private/confidential information being obtained through covert surveillance, the application must be authorised by an Authorised Officer.

14. The Authorising Officer must ensure proper regard is had to necessity and proportionality before any applications are authorised. Stock phrases or cut and paste narrative must be avoided at all times as the use of the same may suggest that insufficient detail and consideration had been given to the particular circumstances of any person likely to be the subject of the claim. This is especially important now reasons must be explained to a Justice of the Peace (JP) Any equipment to be used in any approved surveillance must also be properly controlled, recorded and maintained for audit purposes.

15. The Human Rights Act requires the Council and organisations working on its behalf, pursuant to Article 8 of the European Convention to respect the private and family life of citizens, his home and his correspondence. The European Convention did not however, make this an absolute right, but a qualified right. Accordingly, in certain circumstances the Council may interfere in the citizen's right mentioned above, if such interference is:-

(a) in accordance with the law;
(b) necessary; and
(c) proportionate.

16. The Regulation of Investigatory Powers Act 2000 provides a statutory mechanism for authorising covert Directed Surveillance and the use of Covert Human Intelligence source (CHIS), e.g. undercover agents. It now also permits public authorities to compel telecommunications and postal companies to obtain and release communications data to themselves, in certain circumstances. The Council do not use this facility at present. If there is a desire to use it please contact Legal Services. It seeks to ensure that any interference with the individual's right under Article 8 of the European Convention is necessary and proportionate. In doing so, RIPA seeks to ensure both the public interest and the human rights of individuals are suitably balanced.

17. Directly employed Council Staff and external agencies working for the Council are covered by the Act for the time that they are working for the Council. All external agencies must therefore comply with RIPA and the work carried out by agencies on the Council's behalf must be properly authorised by one of the Council's Authorising Officers. See Appendix 1.

18. If the correct procedures are not followed, evidence may be disallowed by the Courts, a complaint of maladministration could be made to the Ombudsman, and/or the Council could be ordered to pay compensation. Furthermore, breaches would become apparent on inspection from the OSC. Such action would not of course promote the good reputation of the Council and will undoubtedly be the subject of adverse press and media interest. It is essential that that all involved with RIPA comply with this document and any further guidance that may be issued from time to time by Legal Services.

19. A flowchart of the procedures to be followed for Directed Surveillance, CHIS and Communications Data appear at Appendix 2.

C. What RIPA Does and Does Not Do

20. RIPA does:-

- Require prior authorisation of directed surveillance by authorised officers AND a Justice of the Peace (JP)
- Prohibit the Council from carrying out intrusive surveillance
- Compels disclosure of communications data from telecom and postal service providers*
- Require authorisation of the conduct and use of CHIS
- Require safeguards for the conduct and use of CHIS
- Permit the Council to obtain Communications records from Communications service providers.

*NB. Hastings Borough Council has not received any applications requiring authorisation for Communications Data. If you are thinking of making such an application, please contact Legal Services to discuss before submitting an application.

21. RIPA does not:-

- Make unlawful conduct which is otherwise lawful
- Prejudice or dis-apply any existing powers available to the Council to obtain information by any means not involving conduct that may be authorised under this Act. For example, it does not affect the Council's current powers to obtain information via the DVLA or to get information from the Land Registry as to the ownership of a property.

22. If the Authorising Officer or any Applicant is in any doubt he should ask Legal Services before any Directed Surveillance and/or CHIS is authorised, cancelled or rejected.

D. Types of Surveillance

23. Surveillance includes:-

- Monitoring, observing, listening to persons, watching or following their movements, listening to their conversations and other such activities or communications
- Recording anything mentioned above in the course of authorised surveillance
- Surveillance, by or with, the assistance of appropriate surveillance device(s).

Surveillance can be overt or covert.

Overt Surveillance

24. Most of the surveillance carried out by Hastings Borough Council will be done overtly – there will be nothing secretive, clandestine or hidden about it. In many cases, officers will be going about Council business openly.

25. Similarly, surveillance will be overt if the subject has been told it will happen (e.g. where a noise maker is warned (preferably in writing) that noise will be recorded if the noise continues, or where an entertainment licence is issued subject to conditions, and the licensee is told that officers may visit without notice of identifying themselves to the owner/proprietor to check that the conditions are being met).

Covert Surveillance

26. Covert surveillance is carried out in a manner calculated to ensure that the person subject to the surveillance is unaware of it taking place. (Section 26(9)(a) of RIPA). It cannot however be necessary if there is reasonably available an overt means of finding out the information desired.

27. RIPA regulates two types of covert surveillance, (Directed Surveillance and Intrusive Surveillance) and the use of Covert Human Intelligence Sources (CHIS).

Directed Surveillance

28. Directed Surveillance is surveillance which:-

- Can be carried out only for the purpose of preventing or detecting a criminal offence punishable by a maximum term of at least 6 months imprisonment
- Is covert; and
- Is not intrusive surveillance (see definition below – the Council must not carry out any intrusive surveillance or any interference with private property)
- Is not carried out in an immediate response to events which would otherwise make seeking authorisation under the act unreasonable, e.g. spotting something suspicious and continuing to observe it; and
- It is undertaken for the purpose of a specific investigation or operation in a manner likely to obtain private information about an individual (whether or not that person is specifically targeted for purposes of an investigation) (Section 26 (10) of RIPA).

29. Private Information in relation to a person includes any information relating to his private and family life, his home and his correspondence. The fact that Covert Surveillance occurs in a public place or on a 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 undoubtedly result in the obtaining of private information about him/her and others that he/she comes into contact, or associates with.

30. Similarly, although overt town centre CCTV cameras do not formally require authorisation, if the cameras are to be directed for a specific purpose to observe particular individuals, authorisation will be required. The way a person runs his/her business may also reveal information about his or her private life and the private lives of others.

31. For the avoidance of doubt, only those Officers designated and certified to be Authorised Officers for the purpose of RIPA can authorise an application for Directed Surveillance if and only if the RIPA authorisation procedures detailed in this document are followed. If an Authorising Officer had not yet been certified for the purposes of RIPA s/he cannot carry out or approve/reject any action set out in this Corporate Policy and Procedures Document. Once the application is approved by an Authorised Officer the application and any documents in support can only be given effect once an order approving the authorisation or notice has been granted by a Justice of the Peace (JP) at Hastings Magistrates Court.

Intrusive Surveillance (cannot be carried out by the Council)

32. This is when it:-

- Is covert
- Relates to residential premises and/or private vehicles
- Involves the presence of a person in the premises or in the vehicle or is carried out by a surveillance device in the premises/vehicle. Surveillance equipment mounted outside the premises 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/vehicle.

Tracking Devices – Tracking Rubbish

33. Tracking devices to be used in or on skips can be authorised by Authorising Officers provided that the tracking device is disguised as refuse and is not physically attached/affixed to the skip. In the event of there being a requirement that a vehicle tracking device be used and that to install such a device interfered with property not owned by the Council, authorisation will need to be obtained from the police under the Police Act 1997. In either case officers are required to contact Legal Services before authorisation is given.

Necessity and Proportionality

34. Obtaining an authorisation under the 2000 Act, the 1997 Act and 1994 Act will only ensure that there is a justifiable interference with an individual's Article 8 rights if it is necessary and proportionate for these activities to take place. The 2000 Act first requires that the person granting an authorisation believe that the authorisation is necessary in the circumstances of the particular case under section 28(3)(b) of the

2000 Act for directed surveillance. Once necessity is established then proportionality must be considered.

35. The following elements of proportionality should be considered:

- balancing the size and scope of the proposed activity against the gravity and extent of the perceived crime or offence;
- explaining how and why the methods to be adopted will cause the least possible intrusion on the subject and others;
- considering whether the activity is an appropriate use of the legislation and a reasonable way, having considered all reasonable alternatives, of obtaining the necessary result;
- evidencing, as far as reasonably practicable, what other methods had been considered and why they were not implemented

36. In other words this involves the balancing the intrusiveness of the activity on the target subject and others who might be affected by it or against the need for the activity in operational terms. The activity will not be proportionate if it is excessive in the circumstances – each case will be judged on and be unique on its merits – or if the information which is sought could be reasonably be obtained by other less intrusive means. All such activity must be carefully managed to meet the objective in question and must not be arbitrary or unfair. Extra care should also be taken over any publication of the product of the surveillance.

37. It is important that when setting out the proportionality of the surveillance, that the applications include clear statements of the other reasonably possible methods of obtaining the desired information and the reasons why they gave been rejected. This approach will apply, equally, to arguments for the necessity of surveillance. These statements need to convince the JP that the application is necessary and proportionate otherwise it is likely to be refused. It is therefore crucial that the Authorising Officer give particular attention to necessity and proportionality and expresses his own view rather than those explanations given by the applicant.

Further Information

38. Further guidance on surveillance can be found in the Home Office Code of Practice for Covert Surveillance and Property Interference at Appendix 7, and at: www.homeoffice.gov.uk

Confidential Information

39. The authorisation of Directed Surveillance or use of a CHIS likely to obtain Confidential Information or the deployment of a juvenile or vulnerable person (by virtue of mental or other condition) as a CHIS requires authorisation by the Head of Paid Service, or in his/her absence, the acting Head of Paid Service. If there is any doubt regarding sufficiency of rank you should contact the Chief Legal Officer or the Monitoring Officer or Deputy Monitoring Officers who will be able to advise you. Further guidance is available in the Home Office Codes of Practice.

Collateral Intrusion

40. Before authorising surveillance the Authorising Officer should also take into account the risk of intrusion into the privacy of persons other than those who are directly the subjects of the investigation or operation (collateral intrusion). Measures should be taken, wherever practicable, to avoid or minimise unnecessary intrusion into the lives of those not directly connected with the investigation or operation.

41. Those 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. When the original authorisation may not be sufficient, consideration should be given to whether the authorisation needs to be amended and re-authorised or a new authorisation is required. Again, explanation will need to be given to the JPs

42. Further guidance is available in the Home Office Codes of Practice. See Appendix 7 and Appendix 8.

Retention and destruction of product surveillance

43. Where the product of surveillance could be relevant to pending or future criminal or civil proceedings, it should be retained in accordance with established disclosure requirements for a suitable period and subject to review.

44. Were is nothing in RIPA which prevents material obtained from properly authorised surveillance from being used in other investigations. Authorising Officers must ensure therefore, that they follow the procedures for handling, storage and destruction of material obtained through the use of covert surveillance. Authorising Officers must also ensure compliance with the appropriate data protection requirements.

Examples of different types of Surveillance

Type of Surveillance: Overt

45. Examples of Overt types of surveillance:-
    - Police Officer, Street Warden or Parks Ranger on patrol
    - Sign-posted Town Centre CCTV cameras (in normal use)
    - Recording noise coming from outside the premises after the occupier has been warned that this will occur if the noise persists.
    - Most test purchases (where the officer behaves no differently from a normal member of the public).

Type of Surveillance: Covert but not requiring prior authorisation

46. Example of Covert surveillance, not requiring prior authorisation:-
    - CCTV cameras providing general traffic, crime or public safety information.

Type of Surveillance: Directed must be RIPA authorised

47. Examples of Directed surveillance which must be RIPA authorised:- BUT ONLY For the purpose of preventing or detecting a criminal offence

- When the criminal offence to be prevented or detected must be punishable by a maximum term of at least 6 months of imprisonment. An exception is made for RIPA still to be used to prevent or detect the sale of alcohol to underage children although this would apply to Trading Standards

Type of Surveillance: Intrusive – Borough Council cannot do this!

48. Example of Intrusive surveillance:-
    - Planting a listening or other device (bug) in a person's home or in their private vehicle.

E. Conduct and Use of a Covert Human Intelligence Source (CHIS)

Who is a CHIS?

49. A person is a CHIS if he establishes or maintains a personal or other relationship with a person for the covert purpose of facilitating the use of such a relationship to obtain information or to provide access to any information to another person or he covertly discloses information obtained by the use (or as a consequence of the existence) of such a relationship

50. RIPA does not apply in circumstances where members of the public volunteer information to the Council as part of their normal civic duties, or to contact numbers set up to receive information.

What must be authorised?

51. The conduct or use of a CHIS require prior authorisation

- Conduct of a CHIS = establishing or maintaining a persona; or other relationship with a person for the covert purpose of (or is incidental to) obtaining and passing on information
- Use of a CHIS = Actions inducing, asking or assisting a person to act as a CHIS and the decision to use a CHIS in the first place.

52. The Council can use CHIS's if and only if the RIPA procedures, as detailed in this document are followed. Authorisation for a CHIS can be granted for the purpose of preventing or detecting crime or disorder. Again once an authorised officer has approved the application the JP has to hear the application at Hastings Magistrates Court.

NB. Hastings Borough Council has not received any applications requiring authorisation for a CHIS. If you are thinking of making such an application, please contact Legal Services to discuss before submitting an application.

Juvenile Sources

53. Special safeguards apply to the use or conduct of juvenile sources (i.e. under 18 years old). On no occasion can a child under 16 years of age be authorised to give Information against his or her parents. Please seek advice from Legal Services before considering such a request.

    Anti-Social Behaviour activities (e.g. noise, violence etc)

54. Persons who complain about anti-social behaviour and are asked to keep a diary will not normally be a CHIS as they are not required to establish or maintain a relationship for a covert purpose. Recording the level of noise (e.g. the decibel level) will not normally capture private information and therefore does not require authorisation.

55. Recording sound (with a DAT recorder) on private premises could constitute intrusive surveillance unless it is done overtly. For example, it will be possible to record if the

noisemaker is warned that this will occur if the level of noise continues. Placing a stationary or mobile-video camera outside a building to record anti-social behaviour on a residential estate will require prior authorisation.

Further Information

56. Further guidance on CHIS can be found in the Home Office's Code of Practice for Covert Human Intelligence Sources (CHIS) at Appendix 8, and at: www.homeoffice.gov.uk

F. Authorisation Procedures

57. Directed Surveillance and the use of CHIS can only be lawfully carried out if properly authorised, and in strict accordance with the terms of the authorisation. Appendix 2 and Appendix 4 provide flow charts of processes from application/consideration to recording of information and the storage/retention of data obtained.

Authorising Officers

58. Forms can only be signed by Authorising Officers see Appendix 1. The Chief Legal Officer will keep this list up to-date and add, delete or substitute names on request as the service demands.

59. Authorisations under RIPA are separate from delegated authority to act under the Council's scheme of delegation and internal departmental schemes of delegation. All RIPA authorisations save for authorisations to collect communications data under Section 22(3) are for specific investigations only, and must be reviewed, renewed or cancelled once the specific surveillance is complete or about to expire. The authorisations do not lapse with time. Authorisations to collect communications data under Section 22(3) have, as with Section 22 Notices, a life span of one month. However, they can be renewed by serving a new authorisation or notice for a further extension, at any time within the current life of the notice.

Training Records

60. Appropriate training has been given to Authorising Officers and Enforcement personnel. The training is an ongoing programme as and when the service requires. The list of Authorised Officers is kept on the central register at Legal Services. See Appendix 1.

Application Forms

61. Only the RIPA forms set out in this document and available on the Councils website are permitted to be used. Any other forms used will be rejected by the Authorising Officer and/or Legal Services.

Forms Directed Surveillance

62. See Appendix 3a-d:-

3a.	LA1	Application for Authorisation to carry out Directed Surveillance
3b	LA2	Review of a Directed Surveillance Authorisation
3c	LA3	Renewal of a Directed Surveillance Authorisation
3d	LA4	Cancellation of Directed Surveillance Authorisation

Forms Covert Human Intelligence Source (CHIS)

63. See Appendix 5a-d:-

5a	LA5	Application for Authorisation of the Conduct and Use of a CHIS
5b	LA6	Review of a CHIS Authorisation

5c	LA7	Renewal of a CHIS Authorisation
5d	LA8	Cancellation of an Authorisation for the Use or Conduct of a CHIS
2	LA9	Application for Judicial Approval

Grounds for Authorisation

64. Directed Surveillance and the Conduct and Use of the CHIS forms and disclosure of. Communications data notices are to be authorised by Hastings Borough Council only on the grounds of preventing or detecting a criminal offence. No other grounds are available to local authorities. Judicial approval is then required.

Assessing the Application Form

65. Before an Authorising Officer signs a form, s/he must:-

(a) Follow the procedures as laid down in this document and the Home Office Codes of Guidance available on their website. Also, refer to the current Procedures and Guidance available on the Office of Surveillance Commissioners website at: http://surveillancecommissioners.independent.gov.uk If you are in any doubt please contact Legal Services

(b) Satisfy his/herself that a RIPA authorisation is:-

(i) In accordance with the law
(ii) Necessary in the circumstances of the particular case on the grounds mentioned in paragraph 65 above; and
(iii) Proportionate to what it seeks to achieve.

(c) In assessing whether or not the proposed surveillance is proportionate consider whether there are any other non-intrusive means to meet the required aim, if there are none, 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.

(d) Take into account the risk of intrusion into the privacy of persons other than the specified subject of the surveillance (Collateral Intrusion). Measures must be taken wherever practicable to avoid or minimise (so far as is possible) collateral intrusion as the matter may be an aspect of determining proportionality.

Completing the Application Form

66. All forms must be given a unique reference number. Legal Services will issue the unique reference number. A hearing will then be made at Hastings Magistrates Court for the JPs to hear the application. A date for review of the authorisation should be set. The review should take place on that date using the relevant form. A copy of every form/notice and judicial permission must be sent to Legal Services for the Central Register within one week of the relevant authorisation, review, renewal, cancellation or rejection.

Additional Safeguards when Authorising a CHIS

67. When authorising the conduct or use of a CHIS, the Authorising Officer must also:-

    (a) be satisfied that the conduct and/or use of the CHIS is proportionate to what is sought to be achieved

Duration

68. The form must be reviewed in the time stated, renewed and/or cancelled once it is no longer needed. The authorisation to carry out/conduct the surveillance lasts for a maximum of three months (from authorisation) for Directed Surveillance, and 12 months (from authorisation) for a CHIS. However, whether the surveillance is carried out/conducted or not, in the relevant period, does not mean the authorisation is 'spent'. In other words the Forms do not expire, they have to be reviewed, renewed (by application to Court) and/or cancelled once they are no longer required.

69. Notices/Authorities issued under Section 22 compelling disclosure of Communications Data are only valid for one month, but can be renewed for subsequent periods of one month, at any time.

70. Authorisations can be renewed on application to the Court before the maximum period in the authorisation has expired. The Authorising Officer must consider the matter afresh including taking into account the benefits of the surveillance to date, and any collateral intrusion that has occurred. This will need to be explained to the JPs. An authorisation cannot be renewed after it has expired. In such event a fresh authorisation will be necessary on application to the court. The renewal will begin on the day when the authorisation would have expired. In exceptional circumstances, renewals may be granted orally in urgent cases and last for a period of seventy two hours.

G. Record Management

71. A Central Register of all Authorisations, Reviews, Renewals and Cancellations and Rejections will be maintained and monitored by the Chief Legal Officer in regard to Directed Surveillance and CHIS. Authorised Officers will be required to send the Chief Legal Officer a copy of all forms with immediate effect – within one week of authorisation.

72. The Council will retain records for a period of at least three years from the ending of the .The Office of Surveillance Commissioners (OSC) can audit/review the Council's policies and procedures, and individual Authorisations, Reviews, Renewals, Cancellations and Rejections. The documents to be stored will include:-

- A copy of the Forms together with any supplementary documentation and notification of the approval given by the Authorising Officer and Hastings Magistrates Court
- 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 any authorisation, together with the supporting documentation submitted when the renewal was requested
- The date and time when any instruction was given by the Authorising Officer
- The Unique Reference Number (URN) for the authorisation

H. Internet Searches

73. Any investigative search on the Internet must be carried out by searching on the Councils (ask Mark Bourne) Whilst this exercise falls in a non-Ripa category investigations of this type do require the application of the principles of necessity and proportionality and the recognition that collateral intrusion is likely. It may be necessary to conduct a privacy impact assessment. To assist officers in carrying out this kind of surveillance it is required that the form at Appendix 10 is completed. This form should be kept with the working papers of the investigation.

74. Officers are required to comply with the Document Retention policy when destroying data collated in this way. If officers have any questions regarding the use of the intranet and social media please contact the Chief Legal Officer.

I. Concluding Remarks of the Chief Legal Officer

75. Where there is an interference with the right to respect for private life and family guaranteed under Article 8 of the European Convention on Human Rights, and where there is no other source of lawful authority for the interference, or if it is held not to be necessary or proportionate to the circumstances, the consequences of not obtaining or following the correct authorisation procedure set out in RIPA and the document, may be that the action (and the evidence obtained) will be held to be unlawful by the Courts pursuant to Section 6 of the Human Rights Act 1998.

76. Obtaining an authorisation under RIPA and following this document, will ensure, therefore, that the action is carried out in accordance with the law and subject to stringent safeguards against abuse of anyone's human rights.

77. Authorising Officers will be suitably trained and they must exercise their minds every time they are asked to consider a form. They must never sign or rubber stamp form(s) without thinking about their own personal and the Council's responsibilities.

78. Any boxes not needed on the form(s) must be clearly marked as being 'Not Applicable' N/A or a line put through the same. Great care must also be taken to ensure accurate information is used and is inserted in the correct boxes. Reasons for any refusal of an application must be kept on the form and the form retained for future audits.

79. For further advice and assistance on RIPA please contact the Council's Chief Legal Officer

List of Appendices

Appendix 1 List of Authorising Officer Posts
Appendix 2 RIPA Flowchart for Directed Surveillance
Appendix 3 RIPA Forms: Directed Surveillance
- 3a. LA1 Application for Authorisation to carry out Directed Surveillance
- 3b LA2 Review of a Directed Surveillance Authorisation
- 3c LA3 Renewal of a Directed Surveillance Authorisation
- 3d LA4 Cancellation of Directed Surveillance Authorisation

Appendix 4 RIPA Flowchart (CHIS)
Appendix 5 RIPA Forms (CHIS)
- 5a LA5 Application for Authorisation of the Conduct and Use of a CHIS
- 5b LA6 Review of a CHIS Authorisation
- 5c LA7 Renewal of a CHIS Authorisation
- 5d LA8 Cancellation of an Authorisation for the Use or Conduct of a CHIS

Appendix 6 RIPA Flow Chart Directed Surveillance, CHIS or Communications Data
Appendix 7 Home Office Code of Practice for Covert Surveillance and Property Interference
Appendix 8 Home Office Code of Practice for Covert Human Intelligence Sources (CHIS)
Appendix 9 Home Office Guidance to Local Authorities on the Judicial approval process for RIPA and the Crime threshold for Directed Surveillance.