APPENDIX 1

REGULATION OF INVESTIGATORY POWERS

DARLINGTON BOROUGH COUNCIL POLICY 2010-2011

REVIEWED BY CABINET ON: 13th July 2010

CONTENT PAGE

THE REGULATION OF INVESTIGATORY POWERS ACT 2000

Policy Statement

1. Darlington Borough Council will apply the principles of the Regulation of Investigatory Powers Act 2000 (RIPA) to all activities where covert surveillance or covert human intelligence sources are used. In doing so the Council will also take into account their duties under other legislation, in particular the Human Rights Act 1998 and Data Protection Act 1998, and its common law obligations.

Overview of the Act

2. The Act came into force on the 24th September 2000, and aims to balance, in accordance with the European Convention of Human Rights, the right of individuals with the need for law enforcement and security agencies to have powers to perform their roles effectively. The Act and amending Orders allows local authorities to collect evidence of criminal activity lawfully where the investigation requires covert surveillance even where that may lead to them obtaining private information about individuals. The types of surveillance covered by this policy are:

   (a) directed surveillance;
   (b) use and conduct of covert human intelligence sources.

Purpose of the Act

3. RIPA provides a statutory basis for local authorities to authorise the use of directed surveillance and covert human intelligence sources (undercover offices, agents, informants) and accessing communications data. (Darlington Borough Council has a separate Policy in respect of accessing communications data).

4. The Human Rights Act 1998 requires that all actions which may potentially breach an individual's human rights are:-

   (a) proportionate
   (b) necessary
   (c) non-discriminatory
   (d) lawful

5. RIPA provides lawful authority to carry out certain types of surveillance, the carrying out of which could potentially breach an individual's human rights, provided that specified procedures are followed.

6. Failure to comply with RIPA does not mean that an authority's actions in relation to surveillance will be unlawful however it does mean that evidence obtained from surveillance could be inadmissible in court proceedings and jeopardise a successful outcome. Such action could also be open to challenge as a breach of the Human Rights Act and a successful claim for damages could be made against the Council.

Definitions

Private Information

7. "Should be taken generally to include any aspect of a persons private or personal relationship with others, including family and professionals or business relationships" Covert Surveillance and Property Interference Revised Code of Practice 2010 page 12.

Confidential Information

8. Confidential information consists of matters subject to legal privilege, confidential journalistic material, constituent information and confidential personal information which is held in confidence about health, spiritual and/or counselling concerning an individual [whether living or dead] who can be identified from it. Such information requires a higher level of Authority from the Chief Executive. Further information on confidential information is contained in Chapter 4 of the Revised Code of Practice 2010.

Surveillance

9. Monitoring, observing, listening to persons, their movements, their conversations or other activities.

10. Recording anything monitored, observed or listened to in the course of surveillance.

11. Surveillance by or with the assistance of a surveillance device.

Covert Surveillance

12. Surveillance carried out in a manner which is calculated to ensure that the persons subject to the surveillance are unaware that it is or may be taking place.

Intrusive Surveillance

13. (Local Authorities have no power to grant authorisations for intrusive surveillance but it is included here to alert Officers to be aware of inadvertently breaching this rule)

14. Intrusive Surveillance is covered by Section 26(3) of RIPA. Surveillance is intrusive for the purposes of RIPA if, and only if, it is covert surveillance that (a) is carried out in relation to anything taking place on any residential premises or in any private vehicle; And (b) involves the presence of an individual on the premises or in the vehicle or is carried out by means of a surveillance device. Covert surveillance carried out in relation to anything taking place on any residential premises or in any private vehicle. This kind of surveillance may take place by means of either a person or device located inside residential premises or a private vehicle of the person who is subject to the surveillance or by means of a device placed outside which consistently provides a product of equivalent quality and detail as a product which would be obtained from a device located inside.

Residential Premises

15. Includes " any premises as is for the time being occupied or used by any person, however, temporary, for residential purposes or otherwise as living accommodation" Revised Code of Practice 2010 page 16

16. The definition does not include communal areas, front gardens or driveways visable to the public.

Private Vehicles

17. Includes those used primarily for the " private purpose of the person who owns it or a person otherwise having the right to use it" (The Revised Code of Practice 2010) For example a company car.

Directed surveillance

18. Surveillance is "directed" if it is covert, but not intrusive, and is undertaken:-

    (a) for the purposes of a specific investigation or operation;

    (b) in such a manner as is likely to result in the obtaining of private information about a person (whether or not one is specifically identified for the purposes of the investigation).

19. Surveillance will not be directed, and therefore will not require authorisation, if it is done 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 carrying out the surveillance.

20. The Revised Code of Practice 2010 in relation to Directed Surveillance can be found at www.homeoffice.gov.uk/ripa .

Covert Human Intelligence Source

21. A person is identified as a CHIS if he establishes or maintains a personal or other relationship with a person for the covert purpose of facilitating the doing of anything falling within the following two categories:-

(a) he covertly discloses information obtained by the use of such a relationship to obtain information or provide access to any information to another person: or,

(b) he covertly discloses information obtained by the use of such a relationship or as a consequence of the existence of such a relationship.

22. It is possible that persons undertaking test purchases may fall into this category especially if they enter into a prolonged conversation with retail staff. If the purchaser simply enters a shop and purchases an item with the minimum of conversation it is arguable that they are not acting as a CHIS. Such an operation may still require an authorisation for directed surveillance.

23. The Code of Practice relating to Covert Human Intelligence Sources can be found at www.homeoffice.gov.uk.

Revised Code of Practice 2010

24. The Home Office have produced a Code of Practice for Covert Surveillance and Property Interference, this has been revised recently and this Policy has been updated in accordance with the Revised Code. The Revised Code of Practice 2010 provides guidance on the use by public authorities to authorise covert surveillance that is likely to result in obtaining private information about a person. This Revised Code replaces the previous Code of Practice issued in 2002. A copy of the Revised Code of Practice 2010 can be found at www.homeoffice.gov.uk or alternatively contact the Principal Lawyer [People].

Authorisation Procedures

25. Each covert surveillance operation involving directed surveillance and covert human intelligence sources must be authorised either in writing, using the standard forms provided or, in urgent cases, orally.

Oral Authorisations

26. In the case of oral applications a contemporaneous written record must be made of the information provided to the authorising officer and the actions authorised in addition to the reasons for the urgency. A retrospective application need not be completed. However guidance provides that the following information should be

recorded retrospectively as soon as possible following the authorisation being made:

(a) The identities of those subject to surveillance

(b) The nature of the surveillance

(c) Reasons the authorising officer consider that so urgent that oral rather than written authorisation was given

27. Oral authorisations should only be used in cases of urgency. A matter is considered urgent if to wait for written authorisation to be processed is considered likely to endanger life or jeopardise the investigation or operation for which the authorisation was sought.

Written Authorisations

28. In most cases the application will be made in writing by completing the relevant application form and forwarding this to the relevant authorising officer. Authorising officers are those officers listed on page 14 and are either Directors, Heads of Service or Service Managers. Authorising officers can only authorise the use of RIPA if they have completed the SRO approved mandatory training and attended the mandatory training updates.

29. Immediately after authorisation is granted an electronic copy of the form must be sent to the Principal Lawyer [People] with the original being sent in the internal post. This is for the central record. A copy must also be retained by the applicant and authorising officer.

30. Before any authorisation takes place officers must consider whether the surveillance falls under any of the categories covered by RIPA. The Revised Code of Practice 2010 at pages 12-15 outlines those circumstances when a RIPA authorisation is not required or not appropriate.

31. Examples include the following:

(a) The use of CCTV cameras and ANPR systems by public authorities do not usually require RIPA authorisation as they are generally carrying out overt rather than covert surveillance.

(b) If surveillance takes place as an immediate response to events, authorisation will not be required even if the surveillance would generally fall into one of the categories of surveillance covered by RIPA.

Example 1

(i) A CCTV operator observes a crime taking place on his monitor. He would not (unless he was observing a particular property or person as part of a planned surveillance operation) require authorisation to follow the perpetrator with the CCTV camera as he would be acting by way of an immediate response to events.

Example 2

(ii) An officer coincidentally witnesses a private hire vehicle being flagged down by pedestrians. If the officer then observed the driver to investigate whether he would allow the passengers to embark he would be acting by way of an immediate response to events.

32. If the type of surveillance being considered does not fall under RIPA, authorisation will not be required.

33. Even if RIPA does not apply, use of surveillance will still have to be in accordance with the Human Rights Act 1998 and will therefore need to be:

(a) • Proportionate
(b) • Necessary
(c) • Non-discriminatory
(d) • Lawful.

Time Limits

34. Authorisations only remain valid for specific periods and may require renewal or cancellation.

(a) Oral authorisations expire after 72 hours.
(b) Written authorisations will expire after 3 months.

35. Authorisations MUST be cancelled if the conditions are no longer met. Authorisations do not expire when the conditions are no longer met and therefore cancellations are to be made at the earliest opportunity.

Reviews

36. Reviews of Authorisations should take place every four weeks or sooner if the risk of obtaining private information or of collateral intrusion is high and in accordance with the circumstances of the case.

37. A Review will take place by an applicant completing a Review Form which is located on the forms portal of the intranet before the date for review and forward the form to the Authorising Officer for consideration.

38. Records of such decisions should also be placed on the departmental file and copies forwarded electronically [immediately after the review is completed] to the Principal Lawyer (People) for inclusion onto the central file.

Renewals

39. If your authorisation time period is about to end, it will be necessary to complete a renewal form and forward this to the relevant authorising officer who will then consider whether the grounds for authorisation still exist. The copies of the renewal forms must be forwarded electronically [immediately after authorisation is granted] to the Principal Lawyer (People team) for retention in the central record and the original retained for the Department's file.

40. If the authorisation is granted, it will be extended for a further 3 months starting on the date of the day of the old authorisation ended.

Cancellations

41. If the conditions for surveillance being carried out are no longer satisfied, and the authorisation period has not ended, a cancellation form must be completed and all those involved in the surveillance should receive notification of the cancellation, which must be confirmed in writing at the earliest opportunity.

42. Copies of all completed cancellation forms must be forwarded electronically [immediately after cancellation] to the Principal Lawyer (People Team) for retention in the central record within 48 hours from the time of signing the cancellation form. The original form is to be retained for the Department's file.

Records

43. All application forms (whether the application is granted or not), renewal and cancellation forms should be kept on an accessible record within each Department. All records should be kept in a secure place, preferably a locked cabinet or drawer with limited key holders. All authorisations, renewals, cancellations and records of reviews shall be retained for a period of three years commencing on the date the authorisation comes to an end.

44. A Unique Reference Number (URN) should be obtained from the Principal Lawyer (People Team), which holds the centrally retrievable recording system of all RIPA authorisations. This URN will be recorded onto the application for all of the forms completed in respect of a particular authorisation for identification and retrieval purposes.

45. The Centrally Retrievable record of authorisations, renewals and cancellations is maintained by the Principal Lawyer, People Team. The record contains the following information:-

    (a) the type of authorisation
    (b) the date the authorisation was given
    (c) name and rank and grade of the authorising officer
    (d) the URN of the investigation or operation
    (e) the title of the investigation or operation
    (f) whether the urgency provisions were used and if so why
    (g) if the authorisation has been renewed, when it was renewed and who authorised the renewal
    (h) whether the investigation or operation is likely to result in obtaining confidential information
    (i) whether the authorisation was granted by an individual directly involved in the investigation
    (j) the date the authorisation was cancelled

46. To ensure that the Central Retrievable record is up to date, and to allow proper central oversight, it is important that all applications approved and any subsequent renewals, extensions or cancellations are forwarded electronically to the Principal Lawyer (People) as soon as those decision are made.

47. The Central Retrievable record and copy authorisations are kept for a period of three years from the date of the end of the authorisation.

48. All Original and copy documents shall be destroyed after a period of three years from the date the authorisation comes to an end. Regular reviews should take place to ensure that retention and destruction take placed appropriately.

49. In relation to the use of covert human intelligence sources additional records must be maintained (see page 12)

Monitoring and Review

50. Officers who made applications for Authorisations and Authorising Officer should monitor any Authorisation and keep them under review. Consideration should also be given by applicant officers and authorising officers as to whether Authorisations should be cancelled or renewed. Decisions should be recorded in addition to the reasons for those decisions.

51. In addition to the above review mechanism the Senior Responsible Officer (SRO) or his designated officer will review the authorisations held on the central file on a quarterly basis to ensure that the Act is being used consistently with the policy and the policy remains fit for purpose and that authorisation forms are being correctly completed.

52. The Director of Corporate Services is appointed by the Council as the SRO for the purpose of RIPA within the Council. The SRO is responsible for:-

    (a) the integrity of the process in place within the Council to authorise directed surveillance and the use of CHIS
    (b) Compliance with RIPA and its Codes.
    (c) Engagement with the Commissioners and Inspectors when conducting their inspections.
    (d) Where necessary overseeing the implementation of any post-inspection action plans recommended or approved by a Commissioner.
    (e) Ensuring that all authorising officers are of an appropriate standard

53. Elected members will review the RIPA policy annually and will consider internal reports on the use of RIPA at least quarterly. These reports will be completed by the Senior Responsible Officer (SRO) or his designated officer following completion of the quarterly review described above in para 50.

54. Elected members should not be involved in making decisions on specific authorisations.

55. The Office of the Surveillance Commissioner has set up an Inspectorate to monitor the various authorities' compliance with the Act. For local authorities the first point of contact for the Inspectors will be the Chief Legal Officer, (Borough Solicitor) however all Departments' employees and records are likely to be subject to inspection.

Granting Authorisations - Guidance for Authorising Officers

56. Where an application for authorisation is received, it should only be approved where the authorising officer believes the surveillance is:-
    (a) necessary
    (b) Proportionate to what it aims to do
    (c) Non-discriminatory.

57. The authorisation forms contain various sections for completion and, when completed fully, they address all considerations to be taken into account when deciding whether an authorisation can be granted or not. Use the notes below to assist you when applying for authorisations or when asked to authorise applications. Only if all these conditions are satisfied should an application for authorisation be granted.

58. The authorisation form must always be completed and copied. A copy held on a file within the Department. Immediately after an authorisation is granted the form should be forwarded electronically with the original being sent in the internal post to the Principal Lawyer (People Team) for retention on the central file.

Necessity

59. Local authorities are only permitted to obtain such data where it is necessary for the purpose of preventing or detecting crime or of preventing disorder:-

    When completing the application form the applicant should set out:
    (a) The nature of the enquiry or investigation.
    (b) What offences are being investigated?
    (c) When was the complaint received/investigation started?
    (d) Where relevant, outline the intelligence case indicating how the intended surveillance will further the enquiry. This should indicate what steps have already been taken in the investigation to identify any suspects and the evidential value to the investigation of obtaining the information (in other words what will it give you?).
    (e) Where relevant, give the exact date/time/place of the incident under investigation.
    (f) Date of the offence being investigated for which the information is required (or period if relevant). This will demonstrate how collateral intrusion is being minimised by focusing on the offence or search for supporting evidence.
    (g) In long-term or complex investigations it may be appropriate to have an opening paragraph in this section that briefly sets the scene and background which then leads into the specific applicants investigative requirements (in other words; what do you actually want on this occasion).

Proportionality

60. The applicant and authorising officer must also believe that the obtaining of the data is proportionate to what is sought to be achieved by ensuring that the conduct is no more than is required in the circumstances. There must be evidence that consideration has been given by both the applicant and the authorising officer to the issue of proportionality on the written authorisation or the retrospective record of an oral authorisation.

61. "*This involves balancing the seriousness of the intrusion into the privacy of the target of the operation (or other persons who may be affected) against the need fro the activity in investigation and operational terms".*

62. *"The following elements of proportionality should therefore be considered:-*

    (a) Balancing the size and scope of the proposed activity against the gravity and extent of the perceived crime or offence
    (b) Explaining how and why the methods to be adopted will cause the least possible intrusion on the target and others
    (c) 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
    (d) Evidence, as far as practicable, what other methods had been considered and why they were not implemented"
    (Revised *Code of Practice 2010 paras. 3.3-3.6*)

63. If in doubt, should contact the Legal Services Section for assistance to complete the forms.

64. Forms are located on the Forms Portal of the Intranet.

Equipment

65. Each department shall keep a record of equipment held and to be used for the purposes of RIPA. A copy of the list of equipment should be forwarded to the Principal Lawyer (People Team) in order for the central record of all equipment held by the Council to be kept up to date.

66. The equipment is to be held by the individual departments although should be accessible by other departments within the Council in order to carry out the functions under RIPA. Appropriate training is to have been undertaken by the individual installing and using the equipment to ensure that data recorded is fit for purpose and meets the objectives of the investigation.

67. The impact on necessity and/or proportionality will be directed related to the type of equipment used. Any equipment used must be fit for purpose in meeting the objectives of the investigation. It is therefore important for the authorising officer to be informed of what equipment is being used and its capabilities [i.e. range, how its turned on manually or remotely] on the application form so that due consideration can be given when considering whether or not to grant the authorisation. The authorising officer will also need to give consideration and advise how images will be managed, for example images will not be disclosed without first speaking with the data controller to ensure compliance with the appropriate data protection requirements under the Data Protection Act 1998 and any relevant codes of practice produced by the Council.

68. When equipment has been installed a check should be undertaken at least every 48 hours if not daily in order to ensure it remains operational.

69. The Criminal Procedures Investigations Act 1996 Codes of Practice makes provision for the storage and retention of the product of the surveillance. Retention of the investigation data [i.e. images] is to be kept by the relevant department and

in accordance with the Codes of Practice and any relevant policy of that Department.

Covert Human Intelligence Sources (CHIS)

70. If a CHIS is to be used, there are detailed requirements regarding management of their activities. The use of a CHIS who is an adult and not a vulnerable adult can only be authorised by the SRO.

71. You should seek advice from Legal Services when considering the use of a CHIS and before any decisions are made.

72. It is of primary importance when using a CHIS that the Local Authority officers involved comply with the statutory risk assessment requirements specified in section 29 of the Act which are designed for the safety of the individual acting as a CHIS and the protection of the Human Rights of those who may be directly or indirectly involved in the operation. The CHIS must be made aware of any potential risks associated with the role of CHIS.

73. The Code of Practice relating to Covert Human Intelligence Sources can be found at www.homeoffice.gov.uk/ripa . and provides:-

    (a) There will at all times be an officer who has day to day responsibility for dealing with the source and the sources safety and welfare.

    (b) Another officer will have general oversight of the use made of the source.

    (c) An officer will have responsibility for maintaining a record of the use made of the source.

    (d) The records must contain all matters specified by the Secretary of State.

    (e) Records which disclose the identity of the source are not available to persons other than those who need access to them.

74. There are special provisions relating to the use of juveniles as a CHIS

    (a) A CHIS under the age of 16 years old should never be authorised to give information against his parents or anyone with parental responsibility for him.

    (b) The local authority must ensure that an appropriate adult is present at meetings with the CHIS

    (c) Use of a CHIS under the age of eighteen must not be authorised granted or renewed in unless the Local Authority has carried out or updated a risk assessment sufficient to demonstrate that the any risk has been identified and evaluated; that the risk is justified, that the risks have been properly explained and understood by the potential CHIS

    (d) Only the Chief Executive can authorise the use of a juvenile CHIS.

75. A Vulnerable individual is a person who is or may be 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 of himself, or unable to protect himself against significant harm or exploitation. Such a person should only be used as a CHIS in the most exceptional circumstances and only the Chief Executive may authorise use of a vulnerable adult as a CHIS.

76. The Code of Practice details the records which must be kept when using a CHIS. Originals must be hand delivered to the legal services People Team.

77. Each department or section shall nominate an officer who will have responsibility for ensuring that such records are kept and retained and the Borough Solicitor informed of the identity of the designated officer.

78. It should be noted that the Code of Practice states that an officer must not grant authorisation for use of a CHIS unless he believes that there are arrangements in place for ensuring that there is at all times a person with the responsibility for maintaining a record made of the use of the source.

79. Procedures/codes of conduct etc, developed by individual Departments in respect of their operations, which involve the use of a CHIS, must incorporate the requirements of this Policy.

Lawful Business Practice

80. The interception of internet and e-mail communications has to be by or with the consent of a person carrying on a business (which includes the activities of local authorities) for purposes relevant to that person's business and using that business's own telecommunication system. Interceptions are authorised for :-

    (a) monitoring or recording communications
    (b) to establish the existence of facts, to ascertain compliance with regulatory or self-regulatory practices or procedures or to ascertain or demonstrate standards which are or ought to be achieved, (quality control or training);
    (c) in the interests of national security;
    (d) to prevent or detect crime;
    (e) to investigate or detect unauthorised use of telecommunications systems or, to secure or as an inherent part of effective system operation;
    (f) monitoring received communications to determine whether they are business or personal communications;
    (g) monitoring communications made to anonymous telephone helplines.

81. Such interceptions are only allowed if the controller of the telecommunications system on which they are affected has made all reasonable efforts to inform potential users that interceptions may be made. This Council's Internet and E-mail Usage policy does inform employees that internet and e-mail usage is monitored. Please note however that the telephone system is not subject to such monitoring therefore these regulations cannot be used as authorisation to intercept telephone calls.

82. Telephone calls may be intercepted with the consent of one of the parties to the call. However, an authorisation for directed surveillance or for the use of a Covert Human Intelligence Source must first be granted.

83. Local Authorities may not intercept communications where neither party has been made aware that the communication is being monitored.

Darlington Borough Council Designated Authorising Officers

Lesley Blundell - Head of Human Resource Management
Brian James – Head of Corporate Assurance
Bill Westland – Assistant Director – Public Protection
Pamela Ross- Licensing and Car Parking Manager
Cliff Brown - Director of Community Services
Hazel Neasham – Housing Estates Manager
Ian Thompson – Assistant Director Environmental Services
Elizabeth Davison – Assistant Director Finance and IT
Catherine Whitehead – Borough Solicitor
Luke Swinhoe – Head of Legal Services

No officer with direct involvement in an operation should authorise the use of RIPA unless it is unavoidable. If considered to be unavoidable the centrally retrievable record should record that an officer with direct involvement in the operation has authorised the use of RIPA and this authorisation and reasons for it should be highlighted to the commissioner's inspector.