APPENDIX 1

REGULATION OF INVESTIGATORY POWERS

DARLINGTON BOROUGH COUNCIL RIPA POLICY

APPROVED BY CABINET ON: 17 January 2017

CONTENT PAGE

Policy Statement	1
Overview of the Act	1
Purpose of the Act	2
Definitions	2
Does RIPA apply?	5
Restrictions on the use of RIPA	6
Authorisation Procedures	6
Records	8
Monitoring and Review	9
Granting Authorisations-Guidance to officers	11
Equipment	12
CHIS	13
Social Networking Sites and Internet Sites	15
Lawful Business Practice	15
Surveillance outside of RIPA	16
DBC Designated Authorising Officers	17

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 legislation 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.

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 officers, 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 person's private or personal relationship with others, including family and professional or business relationships" Covert Surveillance and Property Interference Revised Code of Practice 2014 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 the physical or mental health or spiritual counselling of a person [whether living or dead] who can be identified from it. Where it is believed that knowledge of confidential information is likely to be acquired, authorisation can only come from the Chief Executive or, in their absence, the Director of Children and Adults Services would deputise for them. Further information on confidential information is contained in Chapter 4 of the Revised Code of Practice 2014.

Surveillance

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

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 any persons who are 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.

Residential Premises

15. “Any premises as is for the time being occupied or used by any person, however temporarily, for residential purposes or otherwise as living accommodation” Revised Code of Practice 2014 page 16

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

Private Vehicles

17. “Used primarily for the private purposes of the person who owns it or a person otherwise having the right to use it” (The Revised Code of Practice 2014). 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 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 2014 in relation to Directed Surveillance can be found at www.gov.uk/government/collections/ripa-codes

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 uses such a relationship to obtain information or to 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. In cases where members of the public contact Council Departments to provide information, consideration will need to be given about whether this person could be a CHIS. The provision of unsolicited historic information (for instance via a fraud hotline) would not be regarded as coming from a CHIS. However if ongoing contact was maintained with an individual who continued to pass information on, consideration must be given about how the information has been obtained (for instance by establishing or maintaining a relationship) and whether the individual should be considered a potential CHIS

24. The Code of Practice relating to Covert Human Intelligence Sources can be found at www.gov.uk/government/collections/ripa-codes

Revised Code of Practice 2014

25. 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 2014 provides guidance on the use by public authorities to authorise covert surveillance that is likely to result in obtaining private information about a person. A copy of the Revised Code of Practice 2014 can be found at

www.gov.uk/government/collections/ripa-codes or alternatively contact the Assistant Director, Law and Governance.

Does RIPA apply?

26. Before any authorisation takes place officers must consider whether the surveillance falls under RIPA. Consideration needs to be given to the changes introduced by the Protection of Freedoms Act 2012 (see paragraph 31 below) and also to circumstances when guidance suggest that RIPA does not apply

27. The Revised Code of Practice 2014 at pages 18-25 outlines those circumstances when a RIPA authorisation is not required or not appropriate.

28. 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 i.e. when they are in public places and are appropriately signed. If this is not the case then authorisation will be required.

    (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.

29. If the type of surveillance being considered does not fall under RIPA, it cannot be authorised. The Council will therefore not be afforded the legal protection that RIPA provides. For this reason, such operations should not be undertaken without the advice of Legal Officers. Please refer to paragraphs 97 to 100 at page 16 of this Policy.

30. 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.

Restrictions on the use of RIPA

31. The Protection of Freedoms Act 2012 (in particular a statutory instrument made under the Act) restricts the use of RIPA to conduct that would constitute a criminal offence which is punishable by a maximum custodial sentence of 6 months or more. This effectively restricts the use of RIPA to circumstances when the conduct is considered to be serious criminal conduct, by reference to sentencing powers.

32. There are some limited exceptions to the 6 month rule, set out in statutory instrument. These are:

a. The sale of alcohol to children (S.146 of the Licensing Act 2003

b. Allowing the sale of alcohol to children (S.147 of the Licensing Act 2003)

c. Persistently selling alcohol to children (S.147A of the Licensing Act 2003)

d. The sale of tobacco to persons under 18 years of age (S.7 Children and Young Persons Act 1933)

33. If RIPA does apply then the investigation will only be lawful if the authorisation procedures set out below are followed.

Authorisation Procedures

34. Each covert surveillance operation involving directed surveillance and covert human intelligence sources must be authorised internally in writing, using the standard forms provided. In addition to the internal authorisation process an application must also be externally approved by a Magistrate. **No investigation can commence until it has been both internally authorised and externally approved by the Court.**

Written Authorisations

35. The application forms are available from the intranet (the forms portal). Each application will have a Unique Reference Number (URN). The URN is obtained from Legal Services, 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.

36. The application will be made in writing (or can be typed) by completing the application form and forwarding this to the relevant authorising officer. Authorising officers are those officers listed on page 15. Authorising officers can only authorise the use of RIPA if they have completed the SRO approved mandatory training and attended the mandatory training updates. Authorisations, unlike applications, should be handwritten and not typed. This is

best practice as, in a typed form, an authorising officer is open to the assertion that they received the authorisation form already completed and merely signed it or that it had been changed retrospectively.

37. Guidance and support in completing the application and authorisation process can be obtained from Legal Services.

38. Immediately after internal authorisation is granted an electronic copy of the form must be sent to the Assistant Director, Law and Governance with the original (with wet signatures) being sent in a confidential envelope via the internal post. This will be retained on the central record. A copy must also be retained by the applicant on the department file.

39. The application for judicial approval by a Magistrate will be made by Legal Services on receipt of the completed internal authorisation.

40. For urgent applications Legal Services should be contacted at the earliest opportunity in order to make urgent arrangements to see a Magistrate. The application form and internal authorisation will still be needed but the time in which to get judicial approval should be reduced.

Time Limits

41. Authorisations only remain valid for specific periods and will require either renewal or cancellation if these periods are to be either increased or reduced. Written authorisations for directed surveillance last for a fixed duration of 3 months and for CHIS they last for a fixed duration of 12 months (or one month in the case of a juvenile CHIS) from the date of the Magistrate's approval.

42. 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. Authorisations must also be cancelled when the fixed duration comes to an end (and renewal is not requested) as authorisations cannot simply expire.

Reviews

43. 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.

44. 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.

45. A copy of the review from should be forwarded electronically [immediately after the review is completed] to the Assistant Director, Law and Governance for inclusion onto the central file. The original form (wet signature) must also be forwarded to the Assistant Director, Law and Governance in the internal post. A copy of the review form should also be kept on the departmental file

Renewals

46. 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. An application for judicial approval by a Magistrate of the internal renewal decision will also be needed. The time in which to get judicial approval will need to be factored in when seeking to get an extension of authorisation. If in the meanwhile the original approval has lapsed no further surveillance should be carried out

47. The copies of the renewal forms must be forwarded electronically [immediately after authorisation is granted] to the Assistant Director, Law and Governance for retention in the central record and the original retained for the Department's file. A copy of the renewal from should be forwarded electronically [immediately after completion] to the Assistant Director, Law and Governance for inclusion onto the central file. The original form (wet signature) must also be forwarded to the Assistant Director, Law and Governance in the internal post. A copy of the renewal form should also be kept on the departmental file

48. Subject to internal authorisation and judicial approval, the surveillance can be extended for a further 3 months and a CHIS can be extended for a further 12 months, starting on the date of the day the old authorisation ended.

Cancellations

49. 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.

50. Copies of all completed cancellation forms must be forwarded electronically [immediately after cancellation] to the Assistant Director, Law and Governance for retention in the central record within 48 hours from the time of signing the cancellation form. The original (with wet signatures) should be sent to Legal Services in the internal post for the central record. A copy must also be retained by the applicant on the department file.

51. Authorisations must also be cancelled when the fixed duration expires (if renewal is not requested) as authorisations do not expire despite the fixed duration coming to an end.

Records

52. The Centrally Retrievable record of authorisations, renewals and cancellations is held in a locked cabinet in Legal Services and overseen by the Assistant Director, Law and Governance. The record for each RIPA application contains the following information:-

    (a) the URN of the investigation or operation
    (b) the title of the investigation or operation

(c) the type of authorisation
(d) the date the authorisation was given
(e) name and rank and grade of the authorising officer
(f) The application for judicial approval and order made
(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

53. 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 sent electronically to the Assistant Director, Law and Governance as soon as those decisions are made. Hard copy original application, extension and cancellation forms (i.e. with wet signatures) must also be forwarded to the Assistant Director, Law and Governance in the internal post. All documents sent by internal post must be marked confidential.

54. The documents in the Central Retrievable record are kept until such time as they have been made available for an OSC inspection and, in any event, for a period of at least three years from the date of the end of the authorisation.

55. 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.

56. Departments should also keep copies of all application forms (whether the application is granted or not), including renewal and cancellation forms on an accessible record. 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.

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

Monitoring and Review

58. 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.

59. 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.

60. The Director of Neighbourhood Services and Resources 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

61. The Assistant Director, Law and Governance is the Co-Ordinating Officer for RIPA. He is responsible for record-keeping; oversight of the applications, authorisations, reviews, renewals and cancellations; organising training; and raising RIPA awareness within the Council.

62. Elected members will review the RIPA policy annually and will consider internal reports on the use of RIPA quarterly. These reports will be completed by the Senior Responsible Officer (SRO) or his designated officer and update members about RIPA usage (or non-usage if there has been no covert surveillance undertaken in a particular quarter of a year), compliance reviews (para 58) and other matters of general relevance concerning RIPA including proposals for legislative change and guidance updates.

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

64. 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 Assistant Director, Law and Governance, however potentially any of the Councils' employees and records could be subject to inspection

Granting Authorisations - Guidance for Authorising Officers

65. Where an application for authorisation is received, it should only be approved where the authorising officer believes the surveillance :-

    (a) Relates to criminal conduct, and is
    (b) necessary
    (c) Proportionate to what it aims to do
    (d) Non-discriminatory.

66. 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.

67. The authorisation form must always be completed and copied. The copy will be held on a file within the Department. Authorising Officers should also retain their own separate copy. Immediately after an authorisation is granted the form should be forwarded electronically to the Assistant Director, Law and Governance with the original form (with wet signatures) sent in the internal post to the Assistant Director, Law and Governance for retention on the central file.

Criminal Conduct

68. The use of RIPA is limited to circumstances when the conduct being investigated is criminal conduct of a certain level of seriousness. Subject to the exceptions set out in the paragraph below, the conduct being investigated must constitute a criminal offence that is punishable by a maximum custodial sentence of 6 months or more.

69. There are some limited exceptions to the 6 month rule. These are:

    a. The sale of alcohol to children (S.146 of the Licensing Act 2003

    b. Allowing the sale of alcohol to children (S.147 of the Licensing Act 2003)

    c. Persistently selling alcohol to children (S.147A of the Licensing Act 2003)

    d. The sale of tobacco to persons under 18 years of age (S.7 Children and Young Persons Act 1933)

Necessity

70. 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).
(h) In the case of applications for directed surveillance authorisations, both the applicant and the authorising officer MUST explain why covert surveillance is a necessary activity for the investigation.

Proportionality

71. 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.

72. "*This involves balancing the seriousness of the intrusion into the privacy of the subject of the operation (or any other person who may be affected) against the need for the activity in investigative and operational terms".*

73. *"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 subject 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) Evidencing, as far as reasonably practicable, what other methods had been considered and why they were not implemented"
(Revised *Code of Practice 2014 paras. 3.3-3.6*)

Equipment

74. 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

Assistant Director, Law and Governance in order for the central record of all equipment held by the Council to be maintained and kept up to date.

75. The equipment is to be held by the individual departments should be accessible by other departments within the Council in order to carry out the functions under RIPA. Appropriate training must be given to the individual installing and using the equipment to ensure that the equipment is correctly installed and that data recorded is fit for purpose and meets the objectives of the investigation.

76. 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.

77. 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.

78. 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)

79. 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 person can authorised by any of the authorising officers. In a case where the proposed CHIS is a juvenile or a vulnerable person, only the Chief Executive can grant an authorisation or, in their absence, the Director of Children and Adults Services would deputise for them and can grant the authorisation instead.

80. Because of the particular requirements when using a CHIS you should seek advice from the Assistant Director, Law and Governance when considering the use of a CHIS and before any decisions are made.

81. 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.

82. The Code of Practice relating to Covert Human Intelligence Sources can be found at www.gov.uk/government/collections/ripa-codes 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.

83. 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 or, in their absence, the Director of Children and Adults Services who would deputise for them, can authorise the use of a juvenile CHIS.

84. 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 or, in the absence of the Chief Executive, only the Director of Children and Adults Services when deputising for them can grant the authorisation instead.

85. The Code of Practice details the records which must be kept when using a CHIS. Originals must be hand delivered to the Litigation Team, Legal Services.

86. Each department or section shall nominate an officer who will have responsibility for ensuring that such records are kept and retained and the

Assistant Director, Law and Governance informed of the identity of the designated officer.

87. 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.

88. 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.

Social Networking Sites and Internet Sites

89. Although social networking and internet sites are easily accessible, if they are going to be used during the course of an investigation, consideration must be given about whether RIPA authorisation should be obtained.

90. Care must be taken to understand how the social media site being used works. Officers must not be tempted to assume that one service provider is the same as another or that the services provided by a single provider are the same.

91. Whilst it is the responsibility of an individual to set privacy settings to protect against unsolicited access to their private information on a social networking site, and even though the data may be deemed published and no longer under the control of the author, it is unwise to regard it as 'open source' or publicly available; the author has a reasonable expectation of privacy if access controls are applied. Where privacy settings are available but not applied the data may be considered open source and an authorisation is not usually required.

92. If it is necessary and proportionate for the Council to covertly breach access controls, the minimum requirement is an authorisation for directed surveillance. An authorisation for the use and conduct of a CHIS is necessary if a relationship is established or maintained by the officer (i.e. the activity is more than mere reading of the site's content). This could occur if an officer covertly asks to become a 'friend' of someone on a social networking site.

93. CHIS authorisation is only required when using an internet trading organisation such as E-Bay or Amazon Marketplace in circumstances when a covert relationship is likely to be formed. The use of disguised purchaser details in a simple, overt, electronic purchase does not require a CHIS authorisation, because no relationship is usually established at this stage.

Lawful Business Practice

94. 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.

95. 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.

96. 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.

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

Surveillance outside of RIPA

98. RIPA provides a lawful means of carrying out directed surveillance and using CHIS.

99. There is case law that suggests that RIPA only applies to circumstances when the local authority is carrying out a core function (these are the specific public functions undertaken by the local authority, for instance a regulatory function). This means that if a matter relates to an ordinary function RIPA does not apply. Accordingly any surveillance activity will be undertaken outside of RIPA (but without the statutory protection afforded by RIPA compliance). In such circumstances the activity will only be lawful if it can be shown that the requirements of the Human Rights Act 1998 have been complied with.

100. Under Article 8 of the European Convention on Human Rights an individual has the right to respect for their private and family life. This is a qualified right, which means that in certain circumstances public authorities can interfere with the private and family life of an individual. Such interference must be proportionate, in accordance with law and necessary to protect national security, public safety or the economic wellbeing of the country; to prevent disorder or crime, protect health or morals, or to protect the rights and freedoms of others.

101. This is a highly technical area. Specific legal advice must be obtained from the Assistant Director, Law and Governance if it is considered that surveillance being contemplated relates to an ordinary function and on any occasion when any surveillance in this category is contemplated.

Darlington Borough Council Designated Authorising Officers:

Ian Thompson – Assistant Director, Community Services
Bill Westland – Assistant Director, Regulatory Services
Pauline Mitchell – Assistant Director, Housing and Building Services
Paul Wildsmith – Director of Neighbourhood Services and Resources

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.