Regulation of Investigatory Powers Act 2000

Mid Sussex District Council

Adopted 24 July 2024

Contents

Introduction to Regulation of Investigatory Powers

1. This policy document is based on the requirements of the Regulation of Investigatory Powers Act 2000 (RIPA), the Protection of Freedoms Act 2012 and the Home Office's Codes of Practice for Covert Surveillance, Covert Human Intelligence Sources (CHIS) and investigation of protected electronic information.

2. Links to the above documents can be found at: -
   - http://www.legislation.gov.uk/ukpga/2000/23/contents
   - http://www.legislation.gov.uk/ukpga/2012/9/contents
   - https://www.gov.uk/government/collections/ripa-codes

Background

3. Surveillance plays a necessary part in modern life. It is used not just in the targeting of criminals, but also as a means of preventing crime and disorder.

4. RIPA introduced a system of authorisation and monitoring of certain surveillance activities, to ensure that the rights of the individual are not unnecessarily compromised, in the pursuance of regulatory compliance. RIPA also requires a similar control and authorisation procedure to be in place for the acquisition of protected electronic information.

5. In addition, the Act established the Investigatory Powers Commissioner's Office (IPCO). IPCO oversees the use of covert investigatory powers by public authorities by carrying out inspections, reviewing applications for warrants, and investigating errors in the use of the powers.

Use of Powers by Mid Sussex District Council

6. In previous years, Mid Sussex District Council ("the Council") used its covert surveillance powers to investigate crime sparingly, and only in the field of benefit fraud. Once the investigation of benefit fraud passed to the Department of Work and Pensions, the Council's use of the powers effectively ceased.

7. There may, however, still be some rare circumstances in which the Council wishes to utilize these powers. Additionally, Council officers need to be aware of the circumstances in which investigative activity would fall under the relevant RIPA provisions and therefore require authorization in order for it to be lawful, not least to avoid inadvertently carrying out such activities.

8. IPCO requires the Council to keep an up-to-date policy, reviewed annually by Members, and to carry out training to keep officers' knowledge current.

What Activities are Regulated?

9. RIPA regulates covert investigative activities. For the Council, this is most likely to be either "Directed Surveillance" or use of a "Covert Human Intelligence Source". Overt investigative activities, such as the overt use of CCTV or ANPR cameras, do not require authorisation.

Directed Surveillance

10. Directed surveillance is:
    - Covert but not intrusive;
    - Conducted for the purpose of a specific investigation or operation;
    - Is likely to result in the obtaining of private information about a person; and
    - Is conducted otherwise than 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 under RIPA to be sought.

Covert Human Intelligence Sources

11. Our investigations may also require the use of Covert Human Intelligence Sources (CHIS). These may be undercover officers, agents, or informants. Such sources may be used by the Council to obtain and pass on information about another person, without their knowledge, as a result of establishing or making use of an existing relationship. Because such activity clearly has implications for personal privacy it is an activity which the legislation regulates. The Council's policy is that a CHIS should be used only rarely, and in exceptional circumstances.

12. If you believe you need to work with a CHIS, you must seek advice from the Council's Senior Responsible Officer (see below) before seeking authorisation. The CHIS must have an appointed controller to oversee their work.

What Happens if I Don't Obtain Authorisation

13. Where authorisation for a regulated activity should have been sought but was not, the Council cannot use the information obtained in legal proceedings. This could compromise the Council's ability to (for example) secure a prosecution in a regulatory matter.

14. A failure to obtain authorization in circumstances where it should have been sought may also lead to an investigation by IPCO.

Policy Statement

15. The Council will not undertake any activity defined within the Regulation of Investigatory Powers Act 2000 without prior authorisation or re-authorisation, from an appropriately trained senior officer, who is empowered to grant such consents, subject to the approval of a Justice of the Peace.

16. **Council officers are NOT legally entitled to authorise *intrusive* surveillance operations.** These are defined as activities using covert surveillance techniques, on residential premises, or in any private vehicle, which involves the use of a surveillance device, or an individual, in such a vehicle or on such premises.

The Senior Responsible Officer

17. The Council has appointed the Assistant Director, Governance, as the Senior Responsible Officer (SRO). As recommended under the Codes of Practice, The SRO is responsible for:
    - the integrity of the process in place within the public authority to authorise directed and intrusive surveillance and interference with property or wireless telegraphy;
    - compliance with Part II of RIPA, and with the Codes of Conduct;
    - oversight of the reporting of errors to the Investigatory Powers Commissioner and the identification of both the cause(s) of errors and the implementation of processes to minimise repetition of errors;
    - engagement with the Investigatory Powers Commissioner and inspectors who support the Commissioner when they conduct their inspections;
    - where necessary, overseeing the implementation of any post-inspection action plans recommended or approved by a Judicial Commissioner, and
    - ensuring that all authorising officers are of an appropriate standard, addressing any recommendations and concerns in the inspection reports prepared by the Investigatory Powers Commissioner

Authorising Officers

18. Under the Council's constitution, the SRO has the authority to appoint Authorising Officers (for surveillance activities) and Designated Persons and Single Points of Contact (for the purposes of access to communications data) under the Act. For such purposes, he has appointed the Chief Executive, Deputy Chief Executive, Director of People and Commercial Services and the Director of Resources and Organisational Development.

19. In circumstances where regulated surveillance activity is likely to involve the acquisition of privileged or confidential information, enhanced authorisation is required and, by law, only the Chief Executive can give authorisation.

The RIPA Co-Ordinating Officer

20. Alex Walker, Solicitor, is the RIPA Co-ordinating Officer responsible for maintaining the Central Record of Authorisations, acting as a gatekeeper by exercising oversight and quality control at the various stages of authorisation, arranging any authorisation hearings at the Magistrates' Court, organising training, and ensuring a high degree of RIPA awareness throughout the Council.

Applications for Authorisation

21. Applications for authorisation of surveillance, the use of a CHIS or the obtaining of protected electronic information will, except in an emergency where legislation permits, be made in writing on the appropriate up-to-date Home Office form available from: https://www.gov.uk/government/collections/ripa-forms—2.

22. The relevant forms are also available on The Wire. The provisions of Section 3 of this Policy must also be followed.

23. The Authorising Officer or Designated Person will not authorise the use of directed covert surveillance techniques, human intelligence sources or access to communications data unless the authorisation can be shown to be *necessary* for the purpose of preventing or detecting crime. In the case of directed surveillance, this must involve the investigation of a crime which attracts a maximum custodial sentence of 6 months or more or relates to the underage sale of alcohol or tobacco.

24. In addition, the Authorising Officer or Designated Person must believe that the surveillance or obtaining of protected electronic information is necessary, reasonable, and proportionate to what it seeks to achieve. In making this judgment, the officer will consider whether the information can be obtained using other methods and whether efforts have been made to reduce the impact of the surveillance on other people who are not the subject of the operation.

Policy on the Recording of Telephone Conversations

25. On occasion, Council officers may need to record telephone conversations to secure evidence. The Council is permitted to record telephone conversations, provided that the parties to that conversation are aware that the conversation is being recorded. In those circumstances, no authorisation is required.

26. If you are unsure whether the parties are aware that the conversation is being recorded, you should take steps to ensure that this is brought to their attention at an early stage in the conversation, for example by telling the other party/ parties overtly that you will be recording the conversation.

Policy on the Use of Social Media for Investigative Purposes

27. Publicly available social media may be used to collect evidence, but officers must use a public, open, clean corporate profile (i.e. a profile which clearly identifies them as a Council officer but does not contain any “posts” or other content) and not use any false identity or attempt to disguise their identity.

28. Individual public profiles should only be viewed on an ad hoc basis. Regular viewing of the same profile will need authorisation. Officers should seek to verify the information collected by other means.

29. Where data has restricted access (e.g. where access is restricted to “friends” on a social networking site) an application for CHIS and, if appropriate, directed surveillance should be made before any attempt to circumvent those access controls is made.

30. Access to open-source material does not require RIPA authorisation unless there are repeated visits to the same site. These normally occur when an attempt is being made to build a profile of the account operator. In that case, directed surveillance authorisation is required.

31. If the privacy controls are breached (e.g. by becoming a “friend”) and a pseudo account is used, concealing the Officer’s identity as a Council employee, then at least directed surveillance authorisation will be required. If direct contact is made with the account owner/operator, and a relationship commences, CHIS authorisation will be required. In the latter case, it is a statutory requirement of RIPA that a Controller, Handler and record keeper are appointed to manage the operation and that a risk assessment is created.

32. Particular regard should be given to the guidance set out at Annex 5 to this Policy.

Obtaining Authorisation

33. The Council’s Constitution provides for the Chief Executive, Deputy Chief Executive and Directors to fulfil the role of Authorising Officer (for the purposes of Directed Surveillance and CHIS authorisation) and Designated Person and Single Point of Contact (for the purposes of access to communications data). The RIPA Co-ordinator shall maintain a register of the names of such Officers.

34. All authorisations must also be approved by a Justice of the Peace.

35. Where a Covert Human Intelligence Source is a juvenile or a vulnerable person, or there is the likelihood that the information acquired will be Confidential Information then the authorisation must be from the Chief Executive or, in their absence, the Deputy Chief Executive and again is subject to the approval of a Justice of the Peace.

36. Authorisations from the Authorising Officer for directed surveillance or the use of a CHIS shall be obtained using the appropriate application form.

37. Applications for access to communications data shall be made to the Designated Person using the appropriate application form) Data can be accessed by a Notice (which is served on the Communications Service Provider (CSP) to produce the data) or by way of an authorisation (which enables persons within a Public Authority to obtain the data). The latter process is unlikely to be used by officers of the Council.

38. Guidance for completing and processing the application forms is attached to this policy at Annexes 1-3. The RIPA Coordinating Officer should be consulted on both draft authorisations and their final wording before authorisation is sought. Once approved by the

Authorising Officer, the RIPA Coordinating Officer will liaise with the Magistrates Court to seek approval of the authorisation by a Justice of the Peace.

Duration of Authorisations

39. A written authorisation (unless renewed) will cease to have effect at the end of the following periods from when it took effect:
    - Directed Surveillance - 3 months;
    - Conduct and use of Covert Human Intelligence Source - 12 months or one month when the CHIS is a juvenile.

40. A notice issued for the production of communication data will remain valid for one month.

Reviews

41. Regular review of authorisations and notices shall be undertaken by the relevant Authorising Officer to assess the need for the surveillance or notice to continue. The results of the review shall be recorded on the Central Record of Authorisations. Where surveillance provides access to Confidential Information or involves collateral intrusion, particular attention shall be given to consideration of the need for surveillance in such circumstances.

42. In each case, the Authorising Officer shall determine how often a review is to take place, and this should be as frequently as is considered necessary and practicable.

Renewals

43. If, at any time, an authorisation or notice would cease to have effect and the Authorising Officer considers it necessary for the authorisation or notice to continue for the purposes for which it was given, he or she may renew it, in writing (subject to the approval of a Justice of the Peace), for a further period of:
    - three months – directed surveillance;
    - twelve months – use of a CHIS
    - one month – access to communications data

44. A renewal takes effect at the time at which the authorisation would have ceased to have effect but for the renewal. A renewal application should not be made until shortly before the authorisation period ends. Any person who would be entitled to grant a new authorisation can renew an authorisation. Authorisation may be renewed more than once provided they continue to meet the criteria for authorisation.

Cancellations

45. The Authorising Officer who granted or last renewed the authorisation or notice must cancel it if he/she is satisfied that the Directed Surveillance, the use or conduct of the Covert Human Intelligence Source or the access to communications data, no longer meets the

criteria for which it was authorised. When the Authorising Officer is no longer available this duty will fall on the person who has taken over the role of Authorising Officer or the person who is acting as Authorising Officer.

46. As soon as the decision is taken that Directed Surveillance should be discontinued or the use or conduct of the Covert Human Intelligence Source, no longer meets the criteria for which it was authorised the instruction must be given to those involved to stop all surveillance of the subject or use of the CHIS. The authorisation does not 'expire' when the activity has been carried out or is deemed no longer necessary. It must be either cancelled or renewed. The date and time when such an instruction was given should be recorded in the central register of authorisations along with the notification of cancellation where relevant.

Obtaining Judicial Approval of Authorisations

47. Authorising Officers must, when making authorisations, be aware that each authorisation (or renewal) will be subject to judicial approval. The Council will be required to make an application to the Magistrates' Court.

48. The Magistrates will approve if, at the date of the grant of authorisation or renewal of an existing authorisation, they are satisfied that:
    (a) there were reasonable grounds for believing that obtaining the covert surveillance or use of a human covert intelligence source was necessary, reasonable, and proportionate and that these grounds remain; and
    (b) the "relevant conditions" were satisfied in relation to the authorisation.

49. The relevant conditions are that:
    (i) the relevant person was designated as an Authorising Officer;
    (ii) it was necessary reasonable and proportionate to believe that using covert surveillance acquisition of communication data or a Covert Human Intelligence Source was necessary, reasonable and that the relevant conditions have been complied with;
    (iii) the grant or renewal of any authorisation or notice was not in breach of any restrictions imposed under section 25(3) of RIPA; and
    (iv) any other conditions provided for by an order made by the Secretary of State were satisfied.

50. If the Magistrates' Court refuses to approve the grant of the authorisation, then it may make an order to quash that authorisation.

51. The Court will also consider whether the "serious crime" threshold has been met in relation to the carrying out of directed surveillance. This threshold is that the directed surveillance is for the purpose of preventing or detecting a criminal offence and meets the following conditions:
    (i) that the criminal offence to be prevented or detected is punishable by a maximum term of a least six months imprisonment: or
    (ii) constitutes an offence under sections 146, 147 or 147A of the Licensing Act 2003 (sale of alcohol to children) or section 7 of the Children and Young Persons Act 1933 (sale of

tobacco to children under 18 years old) or

(iii) constitutes an offence under section 92 Children and Families Act 2014 (sale of nicotine-inhaling products to children under 18 years old) or proxy purchasing of tobacco, including nicotine-inhaling products to children under 18 years old under section 91 Children and Families Act 2014.

52. If the Magistrates' Court refuses to approve the grant of the authorisation, then it may make an order to quash that authorisation.

53. No activity permitted under an authorisation may be undertaken until the approval of the Magistrates' Court has been obtained.

54. To ensure compliance with this requirement, any Authorising Officer who proposes to approve an application for the use of directed surveillance acquisition of communications data or for the use of a CHIS must immediately inform the RIPA Coordinating Officer by telephone or e-mail of the details of the authorisation. The RIPA Coordinating Officer will then make the necessary arrangements for an application to be made to the Magistrates' Court. The Authorising Officer and the Investigating Officer may be required to attend the Magistrates' Court to support the application.

Central Register and Monitoring

55. Any authorisation (including statements in respect of oral authorisations), renewal or cancellation (together with any supporting information relevant to such authorisation or cancellation) of any regulated activity shall be forwarded to the RIPA Co-ordinator within two working days of the date of the application, authorisation, notice, renewal, or cancellation.

56. The RIPA Co-ordinator shall keep a register of the original documents, known as the Central Register of Authorisations.

57. All records shall be kept for at least 3 years and the original authorisations shall be submitted to the RIPA Coordinating Officer and retained with the Central Record of Authorisation.

Training

58. The Authorising Officers, Designated Persons and Single Points of Contact shall be provided with training to ensure awareness of the legislative framework. Single Points of Contact can only be appointed following attendance at a training course accredited by the Home Office and passing a written examination.

Planned and Directed Use of Council CCTV Systems

59. The Council's CCTV surveillance systems shall not be used for Directed Surveillance, without the RIPA Co- Coordinator confirming to the relevant operational staff that a valid

authorisation is in place.

60. When seeking to use the Council's CCTV systems under such an authorisation, regard must be had to the Surveillance Camera Code of Practice.

Kevin Toogood (June 2024)

Glossary

"Confidential information" consists of matters subject to legal privilege, confidential personal information, or confidential journalistic material.

"Directed Surveillance" is defined in section 26 (2) of RIPA as surveillance which is covert, but not intrusive (i.e. takes place on residential premises or in any private vehicle), and undertaken:

(a) for the purpose of specific investigation or specific operation;
(b) in such a manner 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 or operation); and
(c) otherwise, than 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 under Part II of RIPA to be sought for the carrying out of the surveillance.

A person is a "**Covert Human Intelligence Source**" if:
(a) he establishes or maintains a personal or other relationship with a person for the covert purpose of facilitating the doing of anything within paragraph (b) or (c);
(b) he covertly uses such a relationship to obtain information or to provide access to any information to another person; or
(c) he covertly discloses information obtained using such a relationship, or because of the existence of such a relationship.

(See section 26 (8) of RIPA)

"Communications Data" is: -
(a) any traffic data comprised in or attached to a communication (whether by the sender or otherwise) for the purposes of any postal service or telecommunication system by means of which it is being or may be transmitted; (NOT AVAILABLE TO LOCAL AUTHORITIES)
(b) any information which includes none of the contents of a communication (apart from any information falling within paragraph (a) and is about the use made by any person:
    - if any postal service or telecommunications service; or
    - in connection with the provision to or use by any person of any telecommunications service, of any part of a telecommunication system;
(c) any information not falling within paragraph (a) or (b) that is held or obtained, in relation to persons to whom he provides the service, by a person providing a postal service or telecommunications service.

(See section 21(4) of RIPA

"CHIS Controller" means an Officer appointed to oversee the work of a CHIS and ensure the risk assessments are kept up to date.

Annex 1 Guidance on completing Surveillance Forms

Please refer to Covert Surveillance and Property Interference: Code of Practice (Under Section 71 of the Investigatory Powers Act 2000) issued by the Home Office (Revised Code of Practice August 2018)

Details of Applicant

Details of the requesting officer's work address and contact details should be entered.

Details of Application

Give rank or position of authorising officer in accordance with the Regulation of Investigatory Powers (Directed Surveillance and Covert Human Intelligence Sources) Order 2010; No. 521.

Fill in the details of the Authorising Officer.

Purpose of the specific operation or investigation

Outline what the operation is about and what is hoped to be achieved by the investigation. Indicate whether other methods have already been used to obtain this information. Give sufficient details so that the Authorising Officer has enough information to give the Authority e.g. Surveillance at Pelham House and Mr. X".

Describe in detail the surveillance operation to be authorised and the expected duration, including any premises, vehicles, or equipment (e.g. camera, binoculars, recorder) that may be used.

Give as much detail as possible of the action to be taken including which other officers may be employed in the surveillance and their roles. If appropriate append any investigation plan to the application and a map of the location at which the surveillance is to be carried out.

The identities, where known, of those to be subject of the directed surveillance

Explain the information that it is desired to obtain as a result of the directed surveillance.

This information should only be obtained if it furthers the investigation or informs any future actions.

Identify on which grounds the directed surveillance is necessary under section 28(3) of RIPA.

The ONLY grounds for carrying out Directed Surveillance activity is for the purpose of preventing or detecting crime under the Regulation of Investigatory Powers (Directed Surveillance and Covert Human Intelligence Sources) (Amendment) Order 2012 (SI 2012/1500) which came into force on 1 November 2012. It restricts Authorising Officers in a local authority in England or

Wales from authorising the carrying out of directed surveillance unless it is to prevent or detect a criminal offence and meets the following conditions:

(i) that the criminal offence to be prevented or detected is punishable by a maximum term of at least six months imprisonment; or
(ii) constitutes an offence under sections 146, 147 or 147A of the Licensing Act 2003 (sale of alcohol to children) or section 7 of the Children and Young Persons Act 1933 (sale of tobacco to children under 18 years old).

It is therefore essential that Investigating officers consider the penalty attached to the criminal offence which they are investigating, before considering whether it may be possible to obtain an authorisation for directed surveillance.

This can be used in the context of local authority prosecutions, or where an employee is suspected of committing a criminal offence e.g. fraud.

Explain why this directed surveillance is necessary on the grounds you have identified.

Outline what other methods may have been attempted in an effort to obtain the information and why it is now necessary to use surveillance.

Supply details of any potential collateral intrusion and why the intrusion is unavoidable. Describe precautions you will take to minimise collateral intrusion.

Who else will be affected by the surveillance, what steps have been taken to avoid this, and why it is unavoidable.

Explain why the Directed Surveillance is proportionate to what it seeks to achieve. How intrusive might it be on the subject of surveillance or on others? Why is this intrusion outweighed by the need for surveillance in operational terms or can the evidence be obtained by any other means?

If the Directed Surveillance is necessary and reasonable, is it proportionate to what is sought to be achieved by carrying it out? This involves balancing the intrusiveness of the activity on the target and others who may be affected by it against the need for the activity in operational terms. Reasons should be given as to why what is sought justifies the potential intrusion on the individual's personal life and privacy. The activity will not be proportionate if it is excessive in the circumstances of the case or if the information which is sought could reasonably be obtained by other less intrusive means. The following elements of proportionality should therefore 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 responsible way, having considered all reasonable alternatives for obtaining the Evidence;

- Evidencing, as far as reasonably practicable, what other methods have been considered and why they were not implemented (Code para 3.6)

Confidential information.

Is any information of a confidential nature to be obtained? (i.e. communications subject to legal privilege, or communications involving confidential personal information and confidential journalistic material) If so the appropriate level of authorisation must be obtained.

Authorising Officer's comments

Must be completed outlining why it is proportionate and why he/she is satisfied that it is necessary.

Annex 2 Guidance on completing Covert Human Intelligence forms.

Please refer to Covert Human Intelligence Sources: Code of Practice (Pursuant to Section 71 of the Regulations of Investigatory Powers Act 2000) issued by the Home Office.

Details of Application

Authority Required

Fill in details of the Authorising Officer (see paras 3.1 and 3.2 of the Policy)

Where a vulnerable individual or juvenile source is to be used, the authorisation MUST be given by the Chief Executive or in their absence the Assistant Chief Executive.

Describe the purpose of the specific operation or investigation.

Sufficient details so that the Authorising Officer has enough information to give Authority. Outline what the operation is about, and the other methods used already to obtain this information.

Describe in detail the purpose for which the source will be tasked or used.

Give as much detail as possible as to what the use of the source is intended to achieve.

Describe in detail the proposed covert conduct of the source or how the source is to be used.

Describe in detail the role of the source and the circumstances in which the source will be used.

Identify on which grounds the conduct or the use of the source is necessary under Section 29(3) of RIPA.

The ONLY grounds for carrying out a CHIS activity is for the purpose of preventing or detecting crime or of preventing disorder.

This can be used in the context of local authority prosecutions, or where an employee is suspected of committing a criminal offence e.g. fraud.

Explain why this conduct or use of the source is necessary on the grounds you have identified (Code para 3.2).

Outline what other methods may have been attempted to obtain the information and why it is now necessary to use a CHIS for the investigation to proceed.

Supply details of any potential collateral intrusion and why the intrusion is unavoidable. (Code paras 3.8-3.11)

Who else will be affected, what steps have been taken to avoid this, and why it is unavoidable?

Are there any sensitivities in the local community where the source is to be used? Are similar activities being undertaken by other public authorities that could impact the deployment of the source? (see Code 3.17)

Ensure that other authorities such as the police or other council departments are not conducting a parallel investigation or other activity which might be disrupted.

Provide an assessment of the risk to the source in carrying out the proposed conduct. (see Code 6.14)

A risk assessment will have to be carried out to establish the risks to that particular source, taking into account their strengths and weaknesses. The person who has day-to-day responsibility for the source and their security (the 'Handler') and the person responsible for general oversight of the use made of the source (the 'Controller') should be involved in the risk assessment.

Explain why this conduct or use of the source is proportionate to what it seeks to achieve. How intrusive might it be on the subject(s) of surveillance or on others? How is this intrusion outweighed by the need for a source in operational terms, and could the evidence be obtained by any other means? [Code paragraph 3.5]

If the use of a Covert Human Intelligence Source is necessary, is it proportionate to what is sought to be achieved by carrying it out? This involves balancing the intrusiveness of the activity on the target and others who may be affected by it against the need for the activity in operational terms. Reasons should be given as to why what is sought justifies the potential intrusion on the individual's personal life and privacy. The activity will not be proportionate if it is excessive in the circumstances of the case or if the information which is sought could reasonably be obtained by other less intrusive means.

Confidential information (Code para 4.17). Indicate the likelihood of acquiring any confidential information.

Will information of a confidential nature be obtained (i.e. communications subject to legal privilege, or communications involving confidential personal information and confidential journalistic material) if so the appropriate level of authorisation must be obtained (see para 3.2 of the Policy).

Authorising Officer's Comments.

Must be completed outlining why it is proportionate and why he/she is satisfied that it is necessary to use the source and that a proper risk assessment has been carried out.

Annex 3 Guidance on completing access to data forms.

1 - 7 Details of Applicant etc

Details of the requesting officer's Department, Grade and contact details should be entered. The unique reference number at 4 would normally be entered by the SPOC.

Statutory Purpose

The ONLY grounds for accessing communications data are for the purpose of preventing or detecting crime or of preventing disorder.

This can be used in the context of local authority prosecutions, or where an employee is suspected of committing a criminal offence e.g. fraud.

Communications Data

Describe the communications data, specifying, where relevant, any historic or future date(s) and, where appropriate, time period(s).

Indicate the time periods within which the data is required. For example, subscriber details can change over relatively short periods of time. Also billing data can be expensive to retrieve and should only be requested for times relevant to the investigation. It is therefore important to be specific as to the relevant time otherwise there may be collateral intrusion, the data obtained may not be relevant or the cost may be prohibitive. Times should be specified as GMT or BST. If unsure as to whether the data can be obtained from a CSP the SPOC should be consulted.

Necessity

Outline brief details of the investigation, the circumstances leading to the application, the link between the communications data and the subject under investigation, the source of the data and how this data links to the offence or subject under investigation.

Proportionality

Explain what you expect to achieve by obtaining the requested data; what will be done with the data; how it will benefit the investigation and how the level of intrusion is justified when taking into consideration the benefit the data will give to the investigation Also explain why the specific date/timescale has been requested and how this is proportionate to what is trying to be achieved.

Collateral Intrusion

Collateral intrusion is an intrusion into the privacy of innocent third parties. It is important to detail any plan to minimise collateral intrusion. If the subject has been contacted via the

communication service (e.g. telephone number or e-mail) or if it has been used in business correspondence, advertising etc this should be explained as this demonstrates that it is being used by the subject and is therefore unlikely to result in collateral intrusion. Explain how data obtained which refers to third parties will be handled.

Timescale

Indicate whether the application is urgent. The Code of Practice requires CSPs to disclose the data within ten working days (The notice served by the SPOC will remain valid for one month).

The form should then be forwarded to the SPOC officer who will assess and quality control the application. If it meets the legal threshold for obtaining communications data the SPOC will forward it to the appropriate Designated Person.

If rejected, by the Designated Person or the SPOC, the SPOC will retain the application and inform the applicant in writing of the reason(s) for its rejection.

Annex 4 Guidance on Management of Covert Human Intelligence Sources

The Covert Human Intelligence Sources Code of Practice can be found on the Home Office website.

This guidance is taken from Chapter 6 of the Code of Practice.

1. Tasking

1.1 Tasking is the assignment given to the CHIS (i.e. to obtain, provide access to or disclose information). Where the CHIS's task involves establishing or maintaining a personal or other relationship for a covert purpose, authorisation for the use of the CHIS should be obtained in advance.

1.2 Authorisations should not be drawn so narrowly that a separate authorisation is required each time the CHIS is tasked. Rather, an authorisation might cover, in broad terms, the nature of the source's task. If the nature of the task changes significantly, then a new authorisation may need to be sought.

1.3 In the event of any unforeseen action or undertakings during the task, these must be recorded as soon as practicable after the event. If the existing authorisation is insufficient it should either be updated at a review (for minor amendments only) or it should be cancelled and a new authorisation should be obtained before any further such action is carried out.

1.4 Where it is intended to task a CHIS in a significantly greater or different way than previously identified, the Handler and the Controller must refer the proposed tasking to the Authorising Officer and the details of such referrals must be recorded. The Authorising Officer should consider whether the existing authorisation is sufficient or needs to be replaced, which must be done in advance of any tasking.

2. Handlers and controllers

2.1. For each authorised CHIS surveillance, the Authorising Officer shall appoint an appropriate officer of the Authority ('the Handler') to have day-to-day responsibility for:

- Dealing with the CHIS;
- Directing the day-to-day activities of the CHIS;
- Recording the information supplied by the CHIS; and
- Monitoring the CHIS's security and welfare.

2.2. For each authorised CHIS surveillance, the Authorising Officer shall appoint an appropriate officer of the Authority ('the Controller') to be responsible for the management and

supervision of the Handler and general oversight of the use of the CHIS.

3. Joint working

3.1. There are many cases where the activities of a CHIS may provide benefit to more than a single public authority. For example, where a CHIS provides information relating to environmental health issues and offences of criminal damage, in a joint police/ local authority anti-social behaviour operation on a housing estate.

4. Security and Welfare

4.1. Prior to authorising the use or conduct of CHIS, the Authorising Officer should be satisfied that a risk assessment has been carried out. The risk assessment should determine the risk to the CHIS of any tasking and the likely consequences should their identity become known; and should consider the ongoing security and welfare of the CHIS after the cancellation of the authorisation. Consideration should also be given to the management of any requirement to disclose information tending to reveal the existence or identity of the CHIS, or in court.

4.2. The Handler is responsible for bringing to the attention of the Controller any concerns about the personal circumstances of the CHIS, insofar as they might affect:

- the validity of the risk assessment;
- the conduct of the CHIS; and
- the safety and welfare of the CHIS.

Annex 5 Guidance/Policy on Using Social Media and Networking Sites

Using Social Media and Networking Sites in Investigations Policy

A - Introduction
B - Regulation of Investigatory Powers Act 2000 (RIPA)
C - Definition of Social Media
D - Privacy Settings
E - Process to Follow when considering Using Social Media Sites
F - Capturing Evidence
G - Retention and Destruction of Information Obtained
H - Review

A. Introduction

1.0 Social Media has become a significant part of many people's lives. By its very nature, Social Media also often known as Social Networking sites can accumulate a sizable amount of information about a person's life. Their accessibility on mobile devices can also mean that a person's precise location at a given time may also be recorded whenever they interact with a form of Social Media on their devices. This means that incredibly detailed information can be obtained about a person and their activities.

1.1 Social Media can therefore be a very useful tool when investigating alleged offences with a view to bringing a prosecution in the courts. However, there is a danger that the use of Social Media can be abused, which would have an adverse effect damaging a potential prosecution and could even leave the Council open to complainants or criminal charges itself.

1.2 This Policy sets the framework on which the Council may utilise Social Media when conducting investigations into alleged offences. Whilst the use of Social Media to investigate is not automatically considered covert surveillance, its misuse when conducting investigations can mean that it crosses over into the realms of covert and or targeted surveillance, even when that misuse is inadvertent. It is therefore crucial that the provisions of the Regulation of Investigatory Powers Act 2000 (RIPA), as it relates to covert and directed surveillance, are followed at all times when using Social Media information in investigations.

1.3 It is possible for the Council's use of Social Media in investigating potential offences to cross over into becoming unauthorised surveillance, and in so doing, breach a person's right to privacy under Article 8 of the Human Rights Act. Even if surveillance without due authorisation in a particular instance is not illegal, if authorisation is not obtained, the surveillance carried out will not have the protection that RIPA affords and may mean it is rendered inadmissible.

1.4 If is the aim of this Procedure to ensure that investigations involving the use of Social Media are done so lawfully and correctly so as not to interfere with any person's human rights but to ensure that evidence gathered from Social Media is captured and presented to court in the correct manner by obtaining the correct authorisations where necessary.

1.5 Officers who are involved in investigations, into both individuals and businesses they suspect to have committed an offence, should consult Legal Services if they are unsure about any part of this Policy and how it affects their investigative practices.

B. Regulation of Investigatory Powers Act 2000 (RIPA)

2.0 As there is an increase in the use of smartphones and other personal and portable devices, there is a significant amount of information on an individual's Social Media pages. This information might be relevant to an investigation being undertaken by the Council. However unguided and thought-out research into a person's site could fall within the remit of RIPA and therefore require authorisation prior to it being undertaken.

2.1 Officers embarking on any form of investigatory action should always do so with RIPA in mind. Whilst RIPA will not always be relevant to every investigation, it is vital that enforcement officers and those involved in investigations regularly review their conduct with respect to investigatory actions. Any investigation is capable of evolving from one not requiring any RIPA authorisation to one that does at any point.

2.2 This Policy should be read in conjunction with the Council's current RIPA Policy and Procedures as well as statutory codes of practice issued by the secretary of state and the Office of Surveillance Commissioners Guidance.

C. Definition of Social Media

3.0 Social Media also referred to as a Social Network can take many forms. Therefore, it is difficult to provide a definitive list of sites.

3.1 Current examples of popular forms of Social Media include (but the list is not exhaustive and new ones can be created whilst established ones' popularity can wain).

Facebook	Twitter	Instagram
LinkedIn	Pinterest	Reddit

3.2 Social Media will always be a web-based service that allows individuals and/or businesses to construct a public or semi-public profile which contains personal information and is viewable by others, whether accepted as "friends" or otherwise.

3.3 The definition of 'private information' under the Regulation of Investigatory Powers Act (RIPA) includes:

"any information relating to a person's private or family life and 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.

D. Privacy Settings

4.0 The majority of Social Media services will allow its users to decide who can view their activity, and to what degree, through the use of privacy settings. Whilst some users are happy, or indifferent about who can view their information, others prefer to maintain a level of privacy.

4.1 Many users may purposely use Social Media with no privacy settings applied, this could be their intention as they are actively promoting something such as a business or event, and therefore require as many people as possible to be able to view their profile. Others may do so for reasons of self-promotion – this is known as a public profile and the information is "open source".

4.2 Persons operating Social Media without or with limited privacy settings do so at their own risk. Whilst the content or information shared by individuals on Social Media remains the property of that individual, it is nonetheless considered to be in the public domain. Publishing content or information using a public rather than a private setting means that a person is allowing anyone to access that information.

4.3 A private Profile is one set up on Social Media where the individual has set privacy settings and does not want their information open to public view, they will set the privacy settings appropriate to what they require.

4.4 By setting a private profile setting a user does not allow everyone to access their content and respect should be shown to that person's right to privacy under Article 8 of the Human Rights Act. This does not however extend to instances where a third party takes information and shares it on their own profile. So, Person A has a private profile but a friend of theirs Person B takes something from Person A's page and shares it on their public page, this cannot be used from Person A's page but could be from Person B's as they have a public profile.

E. Process to Follow when Considering Using Social Media Sites

5.0 If an individual has a public profile an officer needs to be careful only to gather such information that is relevant to proving the offence they are investigating, if in any doubt seek advice from Legal Services. Even with Public profile sites care must be taken to ensure that the correct authorisation is required if the monitoring of an account becomes planned and directed.

5.1 Officers must not use their own personal or private accounts when accessing social media sites for investigation and evidence-gathering purposes. Only Council accounts should be used. Interaction and conversations of any kind should be avoided.

5.2 Officers should keep in mind that simply using profiles belonging to others, or indeed fake profiles, in order to carry out investigations does not provide them with any form of true anonymity. The location and identity of an officer carrying out a search can be easily traced through tracking IP Addresses and other electronic identifying markers.

5.3 One-off visits or infrequent visits to an individual's Social Media profile spread over time cannot be considered "directed surveillance" for RIPA, repeated or frequent visits may cross over into becoming "directed surveillance" requiring RIPA authorisation. A person's Social Media profile should not, be routinely monitored on a daily or weekly basis in search of updates, as this will require RIPA authorisation. If an officer requires more advice on this they should contact Legal Services.

5.4 Each viewing of a company or individual's social media profile for the purpose of investigation or evidence gathering must be recorded on the case log.

F. Capturing Evidence

6.0 Evidence that is of a readable form, i.e. text, status updates or photographs should be copied directly from the site or captured via a screenshot, onto a hard drive or some other form of storage device and then subsequently printed to a hard copy. The hard copy of evidence should then be exhibited to a prepared witness statement in the normal way.

6.1 If evidence is audio or video content then efforts should be made to download that content onto a hard drive or some other form of storage device such as CD or DVD. Those CDs and/or DVDs should then be exhibited to a suitably prepared witness statement in the normal way. If you have difficulties with this, contact the Council's IT Unit.

6.2 Screenshots – should display the time and date in order to prove when the evidence was captured, without this information, the effectiveness of the evidence is potentially lost as it may not be admissible in court.

6.3 When capturing evidence from a Social Media profile steps should be taken to minimise the collateral damage of inadvertently capturing innocent third parties' information. This might be particularly prevalent on Social Media profiles promoting events.

G. Retention and Destruction of Information Obtained

7.0 Where recorded material (in any form or media) is obtained during the course of an investigation which might be relevant to that investigation, or another investigation, or to pending or future civil or criminal proceedings, then it should be retained in accordance with the Data Protection Act 1998, the Freedom of Information Act 2000 and any other legal requirements including the council's Information asset register and Council's retention schedule. Advice should be sought from the relevant officer at the Council.

H. Review

8.0 This Policy will be reviewed periodically and in line with the Council's RIPA Policy and Procedure to ensure that both documents remain current and compliant with relevant legal requirements and best practice guidance.