

Appendix C

Covert Surveillance and the Acquisition of Communication Data Policy

Contents

Introduction to Covert Surveillance and acquisition of Communications Data.....	2
Policy Statement.....	4
Authorisations.....	5
Duration of Authorisations.....	6
Reviews.....	6
Renewals.....	7
Cancellations.....	7
Central Register of Monitoring.....	7
Planned and Directed Use of Council CCTV Systems.....	8
Obtaining Judicial Approval of Authorisations.....	8
Annex 1 - Surveillance forms.....	11
Annex 2- Covert Human Intelligence Forms.....	12
Annex 3 - Guidance on completing surveillance forms.....	14
Annex 4 - Guidance on completing Covert Human Intelligence forms.....	17
Annex 5 - Guidance on Management of Covert Human Intelligence Sources.....	20
Annex 6 - Guidance/Policy on Using Social Media and Networking Sites.....	22

1. Introduction to Covert Surveillance and acquisition of Communications Data

This policy document is based on the requirements of the Regulation of Investigatory Powers Act 2000 (RIPA), The Protection of Freedom Act 2012 and the Investigatory Powers Act 2016 (IPA).

It also reflects the Home Office's Code of Practices for Directed Surveillance, Covert Human Intelligence Sources and Communications Data.

Harlow District Council (the "Council") has several specific core functions requiring it to investigate the activities of private individuals, groups and organisations within its jurisdiction, for the benefit and protection of the greater public. Such investigations may require the Council to undertake covert investigatory techniques.

Surveillance

1.1 The Council is only permitted to carry out specific types of surveillance by law.

1.2 The Council is permitted to carry out overt surveillance without authorisation, that is surveillance where the person subject to the surveillance will be aware that the surveillance is taking place. For example, the general operation of CCTV cameras with visible signage in a town centre.

1.3 The Council may also carry out covert directed surveillance as defined in RIPA. That is surveillance which is:

1.3.1 carried out in a manner that is calculated to ensure that persons who are subject to the surveillance are unaware that it is or may be taking place;

1.3.2 for the purposes of a specific investigation or a specific operation;

1.3.3 likely to result in obtaining private information about a person, whether or not they are specifically identified for the purposes of the investigation; and

1.3.4 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 to be sought for carrying out the surveillance.

1.4 The Council must not undertake intrusive surveillance. These surveillance activities 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.

Covert Human Intelligence Sources

1.5 The Council may also use a Covert Human Intelligence Source (CHIS) as part of its investigation. A CHIS is a human intelligence source who:

1.5.1 establishes or maintains a personal or other relationship with a person for the covert purpose of facilitating the doing of anything falling within 1.5.2 and 1.5.3

1.5.2 covertly uses a relationship to obtain information or to provide access to any information to another person.

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

1.6 By way of examples which are likely to occur at a local authority, in test purchasing, if the Council deployed an operative to befriend a shopkeeper and gain their trust to try to purchase alcohol underage, a relationship has been established and maintained for a covert purpose and therefore a CHIS authorisation should be obtained.

1.7 If a child is trained simply to make a test purchase of alcohol from a shopkeeper, this exchange will be simply transactional. Without a relationship being formed between the child and the shopkeeper it is unlikely the child would be considered a CHIS and would need authorisation.

1.8 The Council may also receive information from a member of the public about something they have witnessed in their neighbourhood. This member of the public is not a CHIS - they are not passing information obtained as a result of a relationship which has been established for a covert purpose.

1.9 There may however be circumstances where a work colleague volunteers information to the Council about a fellow employee. If the Council asks the work colleague to ascertain further information about the fellow employee, this relationship is being maintained and used for a covert purpose of providing that further information. In this case, it is likely that a CHIS authorisation would be required.

1.10 It is possible that a person may become engaged in the conduct of a CHIS without the Council inducing, asking, or assisting the person to engage in that conduct. However, a CHIS authorisation should be considered, for example, where the Council is aware that an individual is independently maintaining a relationship (i.e. "self-tasking") in order to obtain evidence of criminal activity, and the Council intends to make use of that material for its own investigative purposes.

Communications Data

1.11 Pursuant to the IPA, the Council can also acquire Communications Data which is the 'who', 'when' and 'where' of a communication but not the 'what' (the actual content of what was written). Local authorities are not permitted to intercept the content of any person's communications.

1.11 Part 3 of IPA replaced part 1 chapter 2 of RIPA in relation to the acquisition of Communications Data and puts local authorities on the same standing as the police and law enforcement agencies. Previously local authorities have been limited to obtaining subscriber details (known now as "entity" data) such as the registered user of a telephone number or email address. Under the IPA, local authorities can now also obtain details of in and out call data, and cell site location. This information identifies who a criminal suspect is in communication with and whereabouts the suspect was when they made or received a call, or the location from which they were using an Internet service. This additional data is defined as "events" data.

2. Policy Statement

2.1 The Council will comply with the Regulation of Investigatory Powers Act 2000, (IPA) The Protection of Freedom Act 2012 and the Investigatory Powers Act 2016.

2.2 In complying with this legislation, where necessary, it will seek authorisation to carry out surveillance activity, use a CHIS and/or to acquire Communications Data. Please see section 3 of this Policy for further information on authorisations and how the Council decides whether to use covert surveillance, a CHIS and/or to acquire Communications Data. The Council understands that its authorisations to carry out surveillance activity and to use a CHIS are subject to judicial approval and can only take effect once approval has been granted by a Justice of the Peace.

2.3 In accordance with the legislation, the Council has appointed its Head of Paid Services as Senior Responsible Officer (SRO). The SRO has appointed the Deputy to the Chief Executive and Director of Finance, and the Governance Assistant Directors Authorised Officers.

The Monitoring Officer, is appointed as 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, organising training and ensuring a high degree of RIPA awareness throughout the Council and arranging any authorisation hearings at the Magistrates Court.

2.5 The Authorising Officers shall be provided with training to ensure awareness of the legislative framework.

2.6 It is the policy of the Council to be open and transparent in the way that it works and delivers its services. To that end, a well-publicised Corporate Complaints procedure is in place and information on how to make a complaint to the Investigatory Powers Tribunal will be provided on request by the RIPA Co-ordinator.

2.7 The IPA put in place the Investigatory Powers Commissioner's Office (IPCO) (formerly the Office of Surveillance Commissioners) whose duties are to inspect those public bodies undertaking covert surveillance and acquiring Communications Data. The Investigatory Powers Tribunal now examines complaints where it is alleged that human rights have been infringed.

2.8 We have included separate guidance on the management of CHISs at Annex 5.

2.9 Our approach to investigations involving the use of social media is found in Annex 6

2.10 Elected Members will be provided with an annual report via the corporate leadership team to ensure that the Council is using its policies, procedures and guidance in accordance with the law and to confirm whether this Policy and guidance remains fit for purpose.

3. Authorisations

Directed Surveillance

3.1 The Council can only authorise use of directed surveillance under RIPA to prevent a detect criminal offences that are either punishable by a maximum term of at least 6 months' imprisonment rare related to the underage sale of alcohol and tobacco.

3.2 The Council cannot authorise directed surveillance for the purpose of preventing disorder unless this involves a criminal offence punishable by a maximum term of at least 6 months' imprisonment.

3.3 Directed Surveillance is therefore reserved for more serious cases as long as the other tests are met i.e that it is necessary and proportionate to carry out the surveillance. Low level offences such as littering, dog control and fly posting are unlikely to meet the serious case threshold.

3.4 Directed surveillance authorisations are subject to judicial approval by a Justice of the Peace. This process is explained in section 10 of this Policy.

3.5 The authorisation from the Authorising Office for Directed Surveillance shall be obtained by using the form at Annex 1. Further guidance is also found in Annex 1.

CHIS authorisations

3.6 The Council can only authorise the use of a CHIS if it is for the prevention and detection of crime or the prevention of disorder. It must also be necessary and be proportionate to what is sought to be achieved.

3.7 When considering proportionality, the following matters should be considered:

3.7.1 balancing the size and scope of the proposed activity against the gravity and extent of the perceived crime or offence;

3.7.2 whether the information could be reasonably obtained by other less intrusive means; and

3.7.3 other methods for obtaining the information and why these methods were not implemented.

Where the CHIS 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.

3.8 CHIS authorisations are subject to judicial approval by a Justice of the Peace. This process is explained in section 10 of this Policy.

3.9 The authorisation from the Authorising Officer for the use of a CHIS shall be obtained using the form at Annex 2. Further guidance is also found in Annex 2.

Communications Data

3.10 The IPA has removed the necessity for local authorities to seek the endorsement of a Justice of the Peace when seeking to acquire Communications Data.

3.11 All such applications must now be processed through the National Anti-Fraud Network (NAFN) and will be considered for approval by the independent Office of Communication Data Authorisation (OCDA).

3.13 The Council will not acquire Communications Data unless an application for authorisation is approved both internally, by all Authorising Officer and externally, by the Office for Communications Data Authorisations (OCDA).

3.13 In respect to applications for communications data made under the IPA, the "applicable crime purpose" must be met concerning all applications for both Entity Data and Events Data. The applicable crime purpose is defined differently in relation to each of these data types. Where the Communications Data sought is Entity Data, the applicable crime purpose is the prevention or detection of crime the prevention of disorder. Where the Communication Data is wholly or partly Events Data, the applicable crime purpose is defined as preventing or detecting serious crime defined in s86(2A) IPA (the serious crime threshold). Data relating to Events has the potential to be more intrusive than data relating to Entities.

4. Duration of authorisations

4.1 A written authorisation (unless renewed) will cease to have effect at the end of the following periods from when it took effect:

- a) Directed Surveillance - 3 months
- b) Conduct and use of Covert Human Intelligence Source - 12 months or four months when the CHIS is a juvenile.

4.2 An authorisation to acquire Communications Data will remain in force for one month, unless a further application is made by the Council through NAFN and approved by the OCDA.

5. Reviews

5.1 Regular review of authorisations shall be undertaken by the relevant Authorising Officer to assess the need for the surveillance to continue. The results of the review shall be recorded on the central record of authorisations (see annexes 1 and 2 for review forms). Where surveillance provides access to Confidential Information or involves collateral intrusion, particular attention shall be given to the review for the need for surveillance in such circumstances.

5.2 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.

6. Renewals

6.1 If, at any time, an authorisation would cease to have effect and the Authorising Officer considers it necessary for the authorisation to continue for the purposes for which it was given, he or she may renew it, in writing, for a further period of:-

- three months - directed surveillance (subject to approval from a Justice of the Peace)
- twelve months - use of a CHIS (subject to approval from a Justice of the Peace)
- one month - acquiring of Communications Data.

A renewal takes effect at the time at which the authorisation would have ceased to have effect but for the renewal. An application for renewal should not be made until shortly before the authorisation period is ending. 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.

7. Cancellations

7.1 The Authorising Officer who granted or last renewed the authorisation must cancel it if he/she is satisfied that the Directed Surveillance or the use or conduct of the Covert Human Intelligence Source 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.

7.2 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 and the notification of cancellation where relevant.

7.3 An authorisation to acquire Communications Data may be cancelled at any time by either OCDA or the Council.

8. Central Register and Monitoring

8.1 Applications, authorisations, renewals and cancellations (together with any supporting information) shall be forwarded to the RIPA Co-ordinator within two working days of the date of the application, authorisation, renewal or cancellation.

8.2 The RIPA Co-ordinator shall keep a register of the original documents referred to in paragraph 8.1 above and be involved in, the drafting of those documents and their approval at the Magistrates Court.

8.3 All records will be stored per the Councils retention policy in force from time to time

9. Planned and Directed Use of Council CCTV Systems

9.1 The Council's CCTV surveillance systems shall not be used for Directed Surveillance, without the RIPA Co-ordinator or other senior legal officer confirming to the relevant operational staff that a valid authorisation is in place.

9.2 Also, regard must be had to the provisions of the Protection of Freedoms Act 2012, which required a regulatory framework for surveillance camera systems comprising a code of practice and a surveillance camera commissioner - see the Protection of Freedoms Act 2012 (Code of Practice for Surveillance Camera Systems and Specification of Relevant Authorities) Order 2013.

10. Obtaining Judicial Approval of Authorisations

10.1 Authorising Officers must, when making authorisations, be aware that each authorisation (or renewal of an authorisation) will be subject to judicial approval. The Protection of Freedoms Act 2012 amended RIPA, to require that where an Authorising Officer has granted an authorisation for the use of directed surveillance or for the use of a CHIS, judicial approval will be required. The Council will be required to make an application, without giving notice, to the Magistrates' Court. The Magistrates will give approval if at the date of the grant of authorisation or renewal of an existing authorisation if and only if, 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.

the "relevant conditions" were satisfied in relation to the authorisation. 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 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.

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

10.2 Judicial approval will also review that 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:

a) that the criminal offence to be prevented or detected is punishable by a maximum term of a least six months' imprisonment: or

b) constitutes an offence under sections 146, 147 or 147A of 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

c) 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.

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

10.3 No activity permitted by the authorisation granted by the Authorising Officer may be undertaken until the approval of the Magistrates' Court to that authorisation has been obtained.

To ensure compliance with this requirement, any Authorising Officer who proposes to approve an application for the use of directed surveillance 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 for an order to approve the authorisation 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.

Annex 1 - Surveillance forms

- Application for Authorisation to Carry Out Directed Surveillance

<https://www.gov.uk/government/publications/application-for-use-of-directed-surveillance>

- Review of Directed Surveillance Authorisation

<https://www.gov.uk/government/publications/review-of-use-of-directed-surveillance>

- Cancellation of a Directed Surveillance Authorisation

<https://www.gov.uk/government/publications/cancellation-of-use-of-directed-surveillance-form>

- Application of Renewal of a Directed Surveillance Authorisation

<https://www.gov.uk/government/publications/renewal-form-for-directed-surveillance>

(Always check the Governments site for the most up to date forms and guidance)

<https://www.gov.uk/government/collections/ripa-codes>

Annex 2 - Covert Human Intelligence forms

- Application for Authorisation of the use or conduct of a Covert Human Intelligence Source

<https://www.gov.uk/government/publications/application-for-the-use-of-covert-human-intelligence-sources-chis>

- Review of a Covert Human Intelligence Source (CHIS) Authorisation

Cancellation of an Authorisation for the use of or Conduct of a Covert Human Intelligence Source

<https://www.gov.uk/government/publications/cancellation-of-covert-human-intelligence-sources-chis>

- Application for renewal of a Covert Human Intelligence Source Authorisation

<https://www.gov.uk/government/publications/renewal-of-authorisation-to-use-covert-human-intelligence-sources>

- For guidance Consider the Code of Practice

[https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/949806/Covert Human Intelligence Sources Draft Revised Code of Practice FINAL.pdf](https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/949806/Covert_Human_Intelligence_Sources_Draft_Revised_Code_of_Practice_FINAL.pdf)

Annex 3 - Guidance on completing surveillance forms

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

Details of Applicant

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

Details of Application

1. 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 details of Authorising Officer (see paras 2.3 of Policy).

2. 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".

3. Describe in detail the surveillance operation to be authorized and 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.

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

5. 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

6. 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 Authorizing Officers in a local authority in England or Wales from authorizing the carrying out of directed surveillance unless it is for the purpose of preventing or detecting a criminal offence and meets the following conditions:

- **that the criminal offence to be prevented or detected is punishable by a maximum term of at least six months' imprisonment; or**
- **constitutes an offence under sections 146, 147 or 147A of 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.

7. Explain why this directed surveillance is necessary on the grounds you have identified (code paragraph 3.4).

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

8. Supply details of any potential collateral intrusion and why the intrusion is unavoidable (code paragraphs 3.6 -3.10) Describe precautions you will take to minimize collateral intrusion.

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

9. 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? [Code paragraph 3.5]

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 why what is sought justifies the potential intrusion on the individual's personal life and his 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 of 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)

10. Confidential information. (Code paragraphs 2.1 to 2.12)

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).

12. Authorising Officer's Statement

13. Authorising Officer's comments

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

Annex 4 - 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

1. Details of Application.

Authority Required

Fill in details of Authorising Officer (see paras 2.3 of the Policy)

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

2. Describe the purpose of the specific operation or investigation.

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

3. 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.

4. 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

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

6. 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.

7. 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 done to avoid this, and why it is unavoidable?

8. 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 on 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.

9. 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.

10. 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 why what is sought justifies the potential intrusion on the individual's personal life and his 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.

11. 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).

13. 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 5 - 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 Authorizing Officer and the details of such referrals must be recorded. The Authorizing 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 authorized CHIS surveillance, the Authorizing 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 Authorizing 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 behavior operation on a housing estate.

4. Security and Welfare

4.1. Prior to authorizing the use or conduct of CHIS, the Authorizing 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 6 - Guidance/Policy on Using Social Media and Networking Sites

Using Social Media and Networking Sites in Investigations Policy

Contents Page

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 It 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 mismanaged research into a person's social media presence 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 statutory codes of practice issued by the secretary of state and IPCO's 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
Snapchat	TikTok	Patreon

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 is able to 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 setting 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 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 setting 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 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 account 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 of 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 the purposes of 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 an 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 a memory stick. Those stick(s) should then be exhibited to a suitably prepared witness statement in the normal way. If you have difficulties with this contact the Council's ICT Team.

6.2 Screen shots - 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 2018, 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.