CITY OF Lincoln COUNCIL

REGULATION OF INVESTIGATORY POWERS ACT 2000

POLICY

Document Control

Organisation	City of Lincoln Council
Title	Regulation of Investigatory Powers Act 2000 Policy
Author – name and title	Becky Scott, Legal Services Manager
Owner – name and title	Becky Scott, Legal Services Manager
Date	July 2018
Approvals	Executive
Filename	
Version	V 3.0
Protective Marking	Official
Next Review Date	January 2023

Document Amendment History

Revision	Originator of change	Date of change	Change description
1st Revision	Becky Scott	May 2016	Updating officer details from previous policy and including the CHIS guidance in the policy rather than a separate document
2nd Revision	Becky Scott	July 2018	No changes however reported to Executive
3rd Revision	Becky Scott	January 2021	Changes to authorisations, incorporates technological advances and how to report errors along with some administrative changes

1. GENERAL

1.1 The Regulation of Investigatory Powers Act 2000 (RIPA) came into force on the 25th September 2000. The main purpose of the Act is to ensure that individual's rights are protected whilst allowing law enforcement and security agencies to do their jobs effectively and act proportionately.

1.2 Under Section 28 and 29 of RIPA, it has implications for all staff who investigate suspected criminal offences and other breaches of regulations for which the Council is responsible in regards to Directed Surveillance and Covert Human Intelligence Sources (CHIS).

1.3 This Policy includes the attached 'Guidance to Staff on Use of Covert Human Intelligence Sources (CHIS)' (Appendix A). This together with the Policy outlines the procedures for obtaining authorisations and together these explain:

- the purpose of the Act in relation to the Council's functions
- the circumstances which it applies to
- which authorities can use the powers
- who should authorise each use of power
- the use that can be made of the material gained
- how to make sure that it is complied with
- functions of the Central Register
- process for authorisations
- details for authorisations
- independent judicial oversight
- a means of redress for the individual

The use and conduct of a CHIS will be referred to generally in this Policy, and where appropriate, it is important that officers familiarise themselves with the more detailed Guidance to Staff on use of a CHIS in Appendix A.

1.4 The policies and procedures set out in this Policy replace all those previously in circulation within the Council. This Policy can also be found on Netconsent.

1.5 The City of Lincoln Council is NOT empowered to undertake:

- Intrusive Surveillance or
- Entry onto or interference with property or wireless telegraphy

1.6 The Policy is based on the provisions of RIPA, the Home Office Codes of Practice on Covert Surveillance and Property Interference and the use of CHIS as well as the Home Office Guidance to Local Authorities in England and Wales on the Judicial Approved Process for RIPA and the Crime Threshold for Directed Surveillance. When implementing this Policy, the Officer and the Authorising Officer must ensure that there is compliance with the Home Office Codes of Practice on CHIS and covert surveillance. This can be found at:

https://www.gov.uk/government/publications/covert-surveillance-and-covert-human-intelligence-sources-codes-of-practice

1.7 The provisions of RIPA do not cover authorisations for the use of overt CCTV surveillance systems. Members of the public are aware that such systems are in use for their own protection and to prevent crime. However authorisation maybe required if a CCTV camera is to be used for surveillance as part of a specific investigation or operation otherwise than as an immediate reaction to events. In such circumstances authorisation may either be required by the Council's Authorising Officer or it may come from the police. Where authorisation is given by the police then a record of this authorisation must be kept and officers must ensure that any surveillance is kept within the terms of this authorisation.

1.8 The Covert Surveillance Codes of Practice has kept pace with technology and now acknowledges that Drones can now be used to conduct covert surveillance. Any Council Officers using a drone as part of their duties must adhere to this policy and the ICO's CCTV code of Practice or any Civil Aviation Authority Regulations.

1.9 There is a Flowchart at the end of this Policy to summarise the requirements of the RIPA.

2. THE PURPOSE OF RIPA

2.1 Many teams in the Council find themselves having to undertake investigations of some kind or another from time to time. For some officers it is the essence of their job.

2.2 In the vast majority of cases, investigations can be carried out overtly, i.e. in circumstances where the person under investigation is made aware that he or she is being investigated. Investigations will be carried out overtly wherever possible. Where an operation can be carried out overtly RIPA does not apply.

2.3 However, investigations have the potential to interfere with an individual's human rights, particularly those under Article 8 of the European Convention of Human Rights which provides that "everyone has the right to respect for his private and family life" And where there is likely to be an infringement on these rights, it must be considered necessary and proportionate.

2.4 Article 8 goes on to say that public authorities (which the Council is one) must not interfere with this right unless such interference is;

(a) In accordance with the law
(b) Necessary for certain specified purposes, including public safety, the prevention of disorder and crime, for the protection of health and morals and the protection of the rights and freedom of others.

Local authorities are required to respect the private and family life of citizens, their homes and correspondence in accordance with the Humans Rights Act 1998. This is

a qualified right where interference permissible where it is necessary and proportionate and carried out in accordance with the law. RIPA authorisations amount to an approved interference.

2.5 Section 6 of the Human Rights Act 1998 makes it unlawful for a Council to act in a way which is incompatible with this or any other right under the European Convention. If it does so, section 7 gives the victim the right to bring proceedings against the Council, or challenge its actions in any proceedings brought against him or her. Section 8 empowers the courts to grant an injunction and in exceptional cases to award damages against the Council.

2.6 The main purpose of RIPA is to provide a framework for ensuring that any interference with human rights resulting from the use of the investigatory powers regulated by the Act will be in accordance with the law.

2.7 Proper authorisation of the use of investigatory powers under RIPA will therefore:

- Ensure that the evidence gathered is not challenged in the courts under section 7 of the Human Rights Act 1998
- Protect the Council against claims under section 8 of the Human Rights Act 1998 for acting in a manner incompatible with an individual's rights under the European Convention.

3. WHEN DOES RIPA APPLY?

- Intercepting communications
- Acquiring communications data
- Intrusive surveillance
- Directed surveillance
- The use of covert human intelligence sources
- Gaining access to electronic data protected by encryption

3.1 Council's powers are regulated by Part II of RIPA and are limited to:

- Directed surveillance
- The use of covert human intelligence sources

3.2 "Surveillance" includes;

- monitoring, observing, or listening to persons, their movements, their conversations or other activities or communications
- recording anything monitored, observed, or listened to in the course of surveillance
- surveillance by or with the assistance of a surveillance device (e.g. any apparatus designed or adapted for use in surveillance)

3.3 Surveillance is "**covert surveillance**" if it is carried out in a manner that is calculated to ensure that person being monitored, observed or listened to etc is not aware of it.

3.4 Covert surveillance can be authorised under the act if it is either **Intrusive** or **Directed**.

3.5 Surveillance is "**intrusive"** if it is covert surveillance of anything taking place on residential premises or in a private vehicle AND it involves the investigator being on the premises or using a surveillance device (e.g. a bug or concealed camera). Local Authorities cannot undertake this type of surveillance.

3.6 Surveillance is "**directed**" if it is ALL of the following:

- covert
- not intrusive
- undertaken for a specific investigation or a specific operation
- likely to result in obtaining private information about anyone (NB not necessarily the person targeted)
- planned in advance

3.7 Even carefully directed surveillance can result in private information being obtained about persons other than the target. For example, if premises are under observation because it is suspected that an offence is being committed there, it is likely that private information about innocent visitors to the premises could be obtained as well as information about the suspected offender. Such intrusion on the privacy of people other than the target is referred to as "collateral intrusion". Where collateral intrusion is likely, the surveillance could be "directed surveillance" even if no private information about the suspect is sought or obtained.

3.8 Private information is any information relating to a person's private or family life. It may include personal data, such as names, telephone numbers and address details. It includes (but is not restricted) to information about a person's private or family life and includes the way in which a person conducts his business and professional life. The common sense approach is to interpret the expression broadly and to recognise that it is highly likely that surveillance directed at individuals or groups of individuals will result in obtaining private information about them and/or other people they come into contact with. Where covert surveillance is unlikely to result in obtaining private information about a person (and there will be no interference with Article 8 rights) there is no requirement for authorisation under the Act.

3.9 Surveillance which is not planned in advance, but is undertaken by way of an immediate response to events or circumstances which make it impractical to obtain authorisation, is not regarded as directed surveillance. Thus if an investigating officer notices something suspicious by chance, he or she can continue to keep the suspect under observation without the need for written authorisation. However, returning to the scene subsequently to resume observations would require authorisation.

3.10 It may sometimes be necessary to use the internet to gather information prior to or during an operation which could amount to Directed Surveillance. When the internet is likely to be used as part of an investigation it will be important to consider whether the proposed activity is likely to interfere with an individual's Article 8 rights and should only be used when necessary and proportionate. Where it is considered that

private information is likely to be obtained, an authorisation must be sought. Please see paragraph 18 on social media and Appendix B, which must be adhered to before accessing an individual's social media page.

3.11 Use of Directed Surveillance (or deployment of a CHIS) could potentially be used by the Council in an investigation as a means of obtaining information. Use of either must be authorised. There are designated officers within the Council ('Authorising Officers') who are able to authorise such activity. The authorising officer must consider the detailed legal tests when deciding whether to authorise the covert activity. If the authorising officer does authorise the activity, it is still subject to a judicial process and an application must be made to the Magistrates by Legal Services for approval of the authorisation. No Directed Surveillance or the deployment of a CHIC can take place until Magistrates approval is obtained.

3.12 If you consider that you might wish or need to carry out Directed Surveillance or deploy a CHIS as part of an investigation or even if you are not certain whether the activities you are proposing require a RIPA authorisation, seek advice from Legal Services.

3.13 Most of the surveillance carried out by the Council will be **"Overt."** This means there is nothing secret about it, it is not clandestine or hidden. It will also be overt if the subject has been told it will happen (for example when we investigate noise complaints we write to the noisemaker and tell them that we will be putting in noise monitoring equipment to record the noise.

3.14 Local Authorities can't authorise **"property interference.**" This is entry onto or interference with property or with wireless telegraphy.

3.15 Officers intending to undertake surveillance should therefore consider whether all the criteria set out in the above paragraphs apply to the operation. If so they should obtain authority in advance in accordance with this guidance.

Remember:

- **Overt activities DO NOT need authorisation**
- **Intrusive surveillance CANNOT be authorised**

4. AUTHORISING OFFICERS

4.1 There are comparatively few instances in which Directed Surveillance is likely to be necessary or justified. Most investigations can be carried out by other means. Consequently the Council has designated the following officer to authorise Directed Surveillance:

- **Chief Executive – Angela Andrews**

4.2 Authorised Officers shall have the appropriate training. Additional Authorising Officers will be nominated in writing by the Monitoring Officer following the Monitoring Officer being satisfied that they are appropriately trained to undertake the task.

4.3 An Authorisation acquired in accordance with RIPA, providing the statutory tests are met will provide the Council with a lawful basis in which to carry out covert surveillance activities which are likely to result in the officers involved obtaining private information about an individual.

5. MONITORING OFFICER

5.1 The RIPA Monitoring Officer is Carolyn Wheater (City Solicitor) and the Deputy is Becky Scott (Legal Services Manager)

5.2 The Monitoring Officer's role is to be fully aware of the contents of this policy, it's implementation and updating relevant officers as to the requirements of the legislation.

5.3 The Monitoring Officer will receive and investigate complaints by members of the public who reasonably believe they have been adversely affected by surveillance activities carried out by the Council.

6. APPLYING FOR AUTHORITY

6.1 This is a two-stage process. Firstly, an authorisation must be obtained from the Authorising Officer. Secondly, approval must be obtained from a Justice of the Peace. This involves Legal Services applying to a Magistrates Court.

Written authorisations must be completed whenever an investigation involves the use of Directed Surveillance. This provides lawful authority to carry out Covert Surveillance. Authorisations for Directed Surveillance must be in writing. Authorisation must be sought before any proposed surveillance is undertaken. The Legal Services team will be able to provide advice as to the procedure to be followed when seeking authorisation and will represent the Council at the Magistrates Court to make the application.

6.2 Investigating officers seeking authorisation for Directed Surveillance should do so on the standard forms issued by the Home Office. Two copies of the form should be completed. Those seeking authorisation should ensure that the standard form is the latest version by downloading the form from the Home Office web site www.homeoffice.gov.uk (simply type RIPA forms into the search engine) or checking this with the Legal Services Manager.

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

6.3 Using the standard forms helps both applicants and authorising officers to ensure that the Act is complied with and in particular will focus their attention on the crucial issues of justifying the need for the surveillance and its proportionality to the objective. There are separate forms for issuing, reviewing, renewing and cancelling

authorisations for both Directed Surveillance and the use of CHIS (the forms for a CHIS can be found in Appendix A),

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

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

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

6.4 All applications for authorisation of Directed Surveillance must be in writing and record as a minimum:

- The grounds on which authorisation is sought. Note that the power to authorise surveillance exists only for the prevention and detection of crime and disorder an no other purpose for local authorities.

- An assessment of the Directed Surveillance Crime Threshold. Directed Surveillance can only be authorised under RIPA to prevent or detect criminal offences that are either punishable, whether on summary conviction or indictment, by a minimum term of at least 6 months imprisonment. There are certain specified offences relating to the underage sale of alcohol or tobacco, which are exempt from the Directed Surveillance Crime Threshold. This also means that the Council can't authorise the use of Directed Surveillance to investigate disorder that does not involve criminal offences, or to investigate low level offences, which may include, for example, littering, dog control and fly-posting.

6.5 The person granting an authorisation for Directed Surveillance must believe that this is necessary. If they believe that it is necessary they must also believe that it is proportionate to the aim sought to be achieved by Directed Surveillance. When considering Proportionality the following factors are relevant:-

- Consideration of why the Directed Surveillance is proportionate to what it seeks to achieve.

- An analysis of what other options for gathering the information have been considered and that Directed Surveillance is necessary.

- Balancing the size and scope of the proposed activity against the gravity and extent of the perceived crime or offence;

- Explaining how and why the methods to be adopted will cause the least possible intrusion on the subject and others;

- Considering whether the activity is an appropriate use of the legislation and a reasonable way, having considered all reasonable alternatives, of obtaining the necessary result;

- Evidencing, as far as reasonably practicable, what other methods have been considered and why they were not implemented.

- Balancing the seriousness of the intrusion into the privacy of the subject of the operation (or any other person who may be affected) against the need for the activity in investigative and operational terms and consideration of the potential for Collateral Intrusion and why it is justified.

- The likelihood of acquiring any confidential or privileged material and the details of such material including material subject to legal privilege.

Fundamentally the use of covert surveillance must be proportionate to the issue being investigated.

Authorisation will not be proportionate if it is excessive in the circumstances of the case. Each action authorised should bring an expected benefit to the investigation or operation and should not be disproportionate or arbitrary. No activity will be considered proportionate if the information which is sought could reasonably be obtained by other less intrusive means. All surveillance should be carefully managed to meet the objective in question and must not be arbitrary or unfair.

6.6 When assessing proportionality the following points should be considered:

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

6.7 The following should be considered as best working practices:

- Applications should avoid repetition of information
- Information contained in applications should be limited to that required by the relevant legislation
- Where it is foreseen that other agencies will be involved, these should be detailed in the application
- Authorisations should not generally be sought for activities already authorised following an application by the same or a different Council.

7. GRANTING AUTHORITY

7.1 Before granting authority for Directed Surveillance, the Authorising Officer must believe it is “necessary” in the circumstances of the particular ground only:

- To prevent or detect particular types of criminal offences;

- And these offences must be either punishable, whether on summary conviction or indictment, by a maximum term of at least 6 months or criminal offences related to the underage sale of alcohol and tobacco (it must meet the Directed Surveillance Crime Threshold).

Officers must satisfy themselves that what they are investigating is a criminal offence. If at any time during the investigation it becomes clear that the activity being investigated does not amount to a criminal offence or is a less serious offence which does not meet the threshold the Directed Surveillance Authorisation must be cancelled.

7.2 The test for necessary needs to include a consideration of why it is necessary to use Directed Surveillance. All other grounds identified on the forms must be deleted. Directed surveillance or the use of a CHIS will not be necessary if there are other means of obtaining the required evidence. Therefore consideration must be given to other means of obtaining this evidence before Directed Surveillance or the use of a CHIS is considered and this should be documented.

7.3 As well as believing that the authorisation is necessary, the Authorised Officer will also have to be satisfied that the proposed surveillance is proportionate to the objective.

This is not always an easy test to apply, but as a general rule:

- Covert surveillance should not be used where there are alternative means of obtaining the required information

- Unduly intrusive methods should not be used to obtain information about trivial contravention of offences.

7.4 In this context it is important to bear in mind the risk of Collateral Intrusion as well as the effect on the target.

7.5 An Authorising Officer must give their authorisation in writing. They should not be responsible for authorising operations in which they are directly involved. All authorisations must be recorded in the centrally retrievable record of authorisation.

7.6 A written application for Directed Surveillance should describe any conduct to be authorised and the purpose of the investigation. It should include:

- The reasons why the authorisation is necessary in this particular case and on what grounds
- The nature of the surveillance
- The identities (if known) of the subject of the surveillance
- A summary of the intelligence case and appropriate unique intelligence references where applicable
- An explanation of the information which is desired to be obtained as a result of the surveillance

- The details of any potential Collateral Intrusion and why this intrusion is justified
- The details of any Confidential Information which is likely to be obtained as a consequence of the surveillance
- The reasons why the surveillance is considered proportionate to what it seeks to achieve

A subsequent record should also be made of whether authorisation was given or refused, by whom and the time and date this happened.

7.7 Authorisation will cease to have effect (unless renewed or cancelled) at the end of a period of 3 months beginning on the day the Authorisation was granted.

8. COLLATERAL INTRUSION AND CONFIDENTIAL INFORMATION

8.1 Before authorising Directed Surveillance the Authorising Officer should take into account the risk of obtaining private information about persons who are not the intended subjects of the activity. This is known as Collateral Intrusion.

8.2 Measures should be taken, wherever practicable, to avoid or minimize unnecessary intrusion into the privacy of those who are not the subject of the Directed Surveillance. Where Collateral Intrusion is unavoidable, the activities may still be authorised providing this Collateral Intrusion is considered proportionate to the aims of the intended intrusion. Any Collateral Intrusion should be kept to the minimum necessary to achieve the objectives of the operation. All applications should include an assessment of the risk of any Collateral Intrusion and detail the measures taken to limit this to enable the Authorising Officer to properly consider the proportionality of the surveillance in light of the Collateral Intrusion.

8.3 The risk of Collateral Intrusion must be addressed on the application form. The reasons why Collateral Intrusion is unavoidable and the steps taken to minimise it, must also be set out on the form.

8.4 The form also requires the officer to consider the likelihood of acquiring Confidential Information to be assessed. Confidential Information consists of:

- matters subject to legal privilege (i.e. advice and instructions which are confidential as between legal advisors and their clients)
- confidential personal information about a person's physical or mental health, or spiritual counselling
- confidential journalistic material (i.e. information which a journalist has acquired on a confidential basis)

8.5 If confidential information is likely to be obtained, the Chief Executive is required to be the Authorising Officer.

8.6 Having satisfied themselves about all of the above matters, Authorising Officers must ensure that all the relevant sections of both copies of the application form are

completed and signed. One copy of the completed and signed form should be retained within the department and the original is to go on the Central Register.

9. JUDICIAL APPROVAL

9.1 Under amendments made to the Act by The Protection of Freedoms Act 2012 the Council must now make an application to the Magistrates Court in order to obtain judicial approval. The Council must obtain an order approving the grant or renewal of an authorisation from a Justice of the Peace (JP) before it can take effect.

9.2 No activity permitted by the authorisation granted by the Authorising Officer may be undertaken until the approval of the Magistrates Court of that authorisation has been obtained. An Authorising Officer who intends to approve and application for the use of Directed Surveillance must immediately inform the Monitoring Officer and legal Services in order that the application can be made to the Magistrates Court.

9.3 The JP will consider whether or not the authorisation for the use of Directed Surveillance is necessary and proportionate. They will need to be satisfied that at the time the authorisation was granted or renewed or notice was given or renewed there were reasonable grounds for believing that the authorisation or notice was necessary and proportionate. If the Justice of the Peace is satisfied that the statutory tests have been met and that the use of Directed Surveillance is necessary and proportionate they will issue an order approving the grant or renewal of authorisation as described in the application.

9.4 A RIPA application to a JP is a legal proceeding; this application will be made by Legal Services on behalf of officers with sign off by the RIPA Monitoring Officer. Investigating officers may need to attend and should be prepared to present their evidence to court. The hearing will be a closed one. It is very important that all the evidence relied upon in the application is contained within the forms and supporting papers. They must make the case, it is not sufficient to provide oral evidence where the oral evidence given is not reflected in the papers. Oral evidence should support the documents and should not be used to expand them or present information or evidence that is not already in the papers.

10. DURATION, REVIEW, RENEWAL AND CANCELLATION OF AUTHORISATIONS

10.1 If at any time before an authorisation would cease to have effect, and the Authorising Officer considers it necessary for the authorisation to continue for the purpose for which it was given he/she may approve a renewal in writing for a further period of three months, beginning with the day when the authorisation would have expired but for the renewal.

Authorisations may be renewed more than once, provided they continue to meet the criteria for authorisation.

10.2 Regular reviews of all authorisations should be undertaken to assess the continuing need for Direct Surveillance. The results of the review should be recorded and

retained for 3 years. Where Directed Surveillance involves a high level of Collateral Intrusion or where Confidential Information is likely to be obtained, reviews should be undertaken more frequently.

10.3 Where possible a review should be undertaken by the original Authorising Officer. Where, for whatever reason this is not possible, the review should be undertaken by an officer who would be entitled to grant a new authorisation in the same terms.

10.4 Any proposed or unforeseen changes to the nature or extent of the surveillance operation which may result in further or greater Collateral Intrusion must be brought to the attention of the Authorising Officer through a review. The Authorising Officer must consider whether the proposed changes are proportionate. Any changes must be highlighted at the next renewal.

10.5 Authorisations are of limited duration unless renewed. Their duration is 3 months.

A renewal must be authorised prior to the expiry of the original Authorisation but it runs from the expiry date and time of the original Authorisation. It should not be renewed until shortly before the original Authorisation period is due to expire. Authorisations may be renewed more than once if they are still considered necessary and proportionate and approved by a JP.

As renewals are subject to the approval by the Magistrates Court, Authorising Officers must advise the Monitoring Officer and Legal Services immediately when they are minded to grant a renewal.

Whilst applications for renewals should not be made until shortly before the original authorisations period is due to expire, officers must take into account factors which may delay the renewal process (the availably of the Authorising Officer, Legal Services and court listings).

10.6 Authorising Officers cannot simply allow an authorisation to run its course and expire. An authorisation must be cancelled if it is no longer needed, or if it no longer matches the basis on which it was granted. The need for cancellation may arise before an authorisation is due for review. It is, therefore essential that the investigating officer should draw the attention of the Authorising Officer to any relevant developments and for the Authorising Officer to pro-actively monitor the use being made of the authorisation.

10.7 Formal reviews must be carried out on the date(s) specified in the Authorisation, this should not be later than one months following authorisation. The relevant forms direct Authorising Officers to the matters to be considered on a review. In general terms the considerations are the same as those to be taken into account when first issuing an authorisation.

10.8 An authorisation may be renewed at any time before it expires. All applications for renewal of authorisations for Directed Surveillance should record:

- whether the renewal is the first renewal, or the dates of any previous renewal

- any significant changes to the information on which the authorisation was last issued or renewed
- the reasons why it is necessary to continue with the surveillance
- an estimate of the length of time the surveillance will continue to be necessary.
- the content and value to the investigation of the information so far obtained.
- the results of regular reviews of the investigation or operation.

10.9 Authorisations may be renewed more than once provided that they continue to meet the criteria for Authorisation. Any person who is entitled to grant a new Authorisation can renew an Authorisation. Authorisations must be cancelled if the Directed Surveillance as a whole no longer meets the criteria upon which it was authorised.

10.10 All reviews, cancellations and renewals must be recorded on the relevant forms, which should be completed in duplicate. The forms direct Authorising Officers towards the relevant considerations to be taken into account.

10.11 Reviews, renewals and cancellations should be carried out by the Authorised Officer who first issued the relevant Authorisation. The details of any renewal should be centrally recorded.

10.12 Authorising Officers are required to ensure that:

- Authorisations have been properly cancelled at the end of the period of surveillance
- Surveillance does not continue beyond the authorisation period
- Current authorisations are regularly reviewed
- Ensure the timely destruction of the results of surveillance operations

11. CENTRAL REGISTER

11.1 A centrally retrievable record of all authorisations should be held by the Council and updated whenever an Authorisation is granted, renewed or cancelled. This information must be held for three years from the end of each Authorisation. If there is reason to believe that any of the information obtained as a result of the authorisation might be relevant to further civil or criminal proceedings then this should not be destroyed but should be retained in accordance with established disclosure requirements. The record should be made available to the relevant Commissioner or Inspector from the Office of Surveillance Commissioners upon request.

11.2 The record must contain the following information:

- The date that the Authorisation was given
- The name and position of the Authorising Officer
- The unique reference number (URN) of the investigation, its title and a brief description of the names and subjects (if known)

- The details of the attendance at the Magistrates, the date of the attendance, the determining Magistrate, the decision of the court and the time and date of the decision
- The date of any reviews
- If the Authorisation has been renewed when it was renewed, who authorised the renewal (name and position of the officer)
- Whether the investigation is likely to result in obtaining any Confidential Information
- The date the Authorisation was cancelled.
- Where the application is refused, the grounds or reasons for refusal given by the Authorising Officer or the Justice of the Peace.

11.3 The following documentation should also be centrally retrievable for at least three years following the end of the Authorisation:

- A copy of the Application and a copy of the Authorisation with any supplementary documentation and notification of the approval given by the Authorising Officer.
- A record of the period over which the surveillance has taken place
- The frequency of the reviews prescribed by the Authorising Officer
- A record of the results of each review of the Authorisation
- A copy of any renewal of an Authorisation with any supporting documents submitted when the renewal was requested.
- Date and time when any instruction to cease surveillance was given
- A copy of the order approving or otherwise the grant for renewal of an Authorisation from a JP.

11.4 The Central Register is kept by the RIPA Monitoring Officer, who will also retain an excel spreadsheet of the Central Register. The RIPA Monitoring Officer is responsible for maintaining the Central Register.

12. KEEPING RECORDS

12.1 Quite apart from the statutory requirement that Authorisations should be in writing, there is self-evidently a need to keep proper records so that the protection of the Act can be relied upon in any legal proceedings if needs be.

12.2 As outlined earlier, two copies of every Authorisation, review, renewal or cancellation should be completed. One should be retained by the department and the original sent to the RIPA Monitoring Officer, to be put onto the Central Register. The Authorising Officer is responsible personally for ensuring that copies of those documents are sent to the RIPA Monitoring Officer, within one week.

12.3 Forms should be handed over personally or sent in a sealed envelope marked “Private and Confidential”.

12.4 The handling, storage and destruction of material obtained through an operation must be done so in accordance with the requirements of the General Data Protection Regulation and the Council's policies.

12.5 Material gathered under RIPA through Directed Surveillance which has been properly Authorised can be used to further other investigations.

12.6 Each service department undertaking Directed Surveillance must ensure that adequate arrangements are in place for the secure handling, storage and destruction of material obtained through the use of covert surveillance.

13. HEALTH AND SAFETY

13.1 Authorising Officers are reminded of the need to ensure that the health and safety implications of undertaking investigations are taken into account.

13.2 This, of course, applies whether or not Covert Surveillance is taking place, but in certain circumstances the level of risk to employees may be increased by covert activity. The risk must be properly assessed and steps taken to minimise it.

14. WORKING WITH/THROUGH OTHER AGENCIES

14.1 In certain circumstances it may be necessary for the Council to work with other agencies on a surveillance operation. When this is the case the Council should try to avoid duplication of Authorisations. Where there has been duplication this will not affect the lawfulness of the activities conducted.

14.2 When another agency has been instructed on behalf of the Council to undertake any action under RIPA, this policy and the forms in it must be used (as per normal procedure) and the agency advised or kept informed, as necessary, of the various requirements.

14.3 When another agency (e.g. the Police, Customs and Excise, Inland Revenue etc); -

- wish to use the Council's resources (e.g. CCTV) that agency must use its own RIPA procedures and before an officer agrees to allow the Council's resources to be used by any agency they must obtain a copy of that agency's RIPA form for the record (a copy of which must be passed to the RIPA Monitoring Officer for the Central Register).

- wish to use the Council's premises for their own RIPA action the officer should, normally co-operate with the same, unless there are security or other good operational or managerial reasons as to why the City Council's premises should not be used for the agency's activities. Suitable insurance or other appropriate indemnities may be sought, if necessary, from the agency. In such cases the Council's own RIPA forms should not be used as the Council's role is simply to assist in the RIPA activity.

14.4 If the Police or other agency want to use the Council resources for general surveillance, as opposed to specific RIPA operations, an appropriate letter requesting the proposed use, extent of remit, duration, who will be undertaking the general surveillance and the purpose of it must be obtained from the Police or other Agency before any Council resources are made available for the proposed use. If in doubt please consult with the RIPA Monitoring Officer or the Legal Services Manager at the earliest opportunity.

15. TRAINING

15.1 The RIPA Monitoring Officer should ensure that all officers who are required to undertake investigations receive relevant RIPA training and appropriate refresher training. However, any investigating officer who feels that they need further training or refresher training should raise this with their supervisor at the earliest opportunity. It is the responsibility of all investigating officers to ensure that they keep up to date with any developments or changes to RIPA. In house training can be sought by contacting Legal Services.

16. SENIOR RESPONSIBLE OFFICER (SRO)

16.1 The Council has appointed the City Solicitor as the SRO who is responsible for the following:-

- The integrity of the process in place within the Council to authorise Directed Surveillance.
- For ensuring that all Authorising Officers are of an appropriate standard in light of any recommendations in the inspection reports prepared by the Office of the Surveillance Commissioner.
- Compliance with Part II of the 2000 Act, Part III of the 1997 Act and with this code;
- Engagement with the Commissioners and Inspectors when they conduct their inspections, and
- Address any post inspection action plans recommended or approved by a Commissioner.

17. REVIEW AND PUBLICATION

17.1 The Policy will be reviewed annually and any changes presented to the Executive on an annual basis to comply with the Codes, the legislation and to ensure that it is being used consistently. It may be amended from time to time in light of any developments in the law and experience of the operation to ensure that it remains fit for purpose. Staff are encouraged to raise any issues they may have with the Legal Services Manager.

17.2 The Executive shall review the Council's use of RIPA annually in accordance with the Code of Practice on Covert Surveillance and Property Interference.

18. SOCIAL MEDIA

18.1 It is important to be aware that the use of social media in an investigation could, depending on how it is used and the type of information likely to be obtained, constitute covert activity that requires authorisation under RIPA.

18.2 Researching 'open source' material would not require authorisation but return visits to these sites in order to build up a profile could change this position and may constitute Directed Surveillance and need an authorisation. As such before any integration of social media is undertaken a social media access request form (attached at Appendix B) must be completed and signed by one of the Council's solicitors.

18.3 Officers should not use false personae (a false social media profile or handle) or their own social media to undertake any authorised social media searches. The Council's own social media accounts must be used for this.

19. ERRORS AND BREACHES OF RIPA

19.1 An error must be reported if it is a Relevant Error (as defined under section 231(9)_RIPA. An example of Relevant Errors occurring would include circumstances where Surveillance or the use of a CHIS has taken place without the lawful authority.

19.2 All Relevant Errors made by the Council of which it is aware must be reported to the IPC as soon as reasonably practicable and no later than 10 working days.

19.3 Once the error has been identified, the Council must take steps to confirm the fact of an error as quickly as it is reasonably practicable to do so. Where it is subsequently confirmed that an error has occurred and that the error is notified to the Commissioner, the Council must also inform the commissioner of when it was initially identified that an error may have taken place.

19.4 A full report must be sent to the Investigatory Powers Commissioner as soon as reasonably practicable in relation to any relevant error, including details of the error. The report should include information on the cause of the error, the amount of surveillance conducted and any material obtained or disclosed, any collateral intrusion, any analysis of the action taken, whether any material has been retained or destroyed and a summary of the steps taken to prevent recurrence.

19.5 If the Investigatory Powers Commission considers the error to be a serious error and that it is in the public interest for the person concerned to be informed of the error, they must inform them. An error is a serious error where it is considered to have caused significant prejudice to the person concerned. When deciding whether it is in the public interest for the person concerned to be informed of the error, the Commissioner must in particular consider:

- The seriousness of the error and its effect on the person concerned
- The extent to which disclosing the error would contravene the public interest and be prejudicial to: national security, the prevention or detection of serious crime, the economic well-being of the United Kingdom or the continued discharge of function of any of the security and intelligence services.

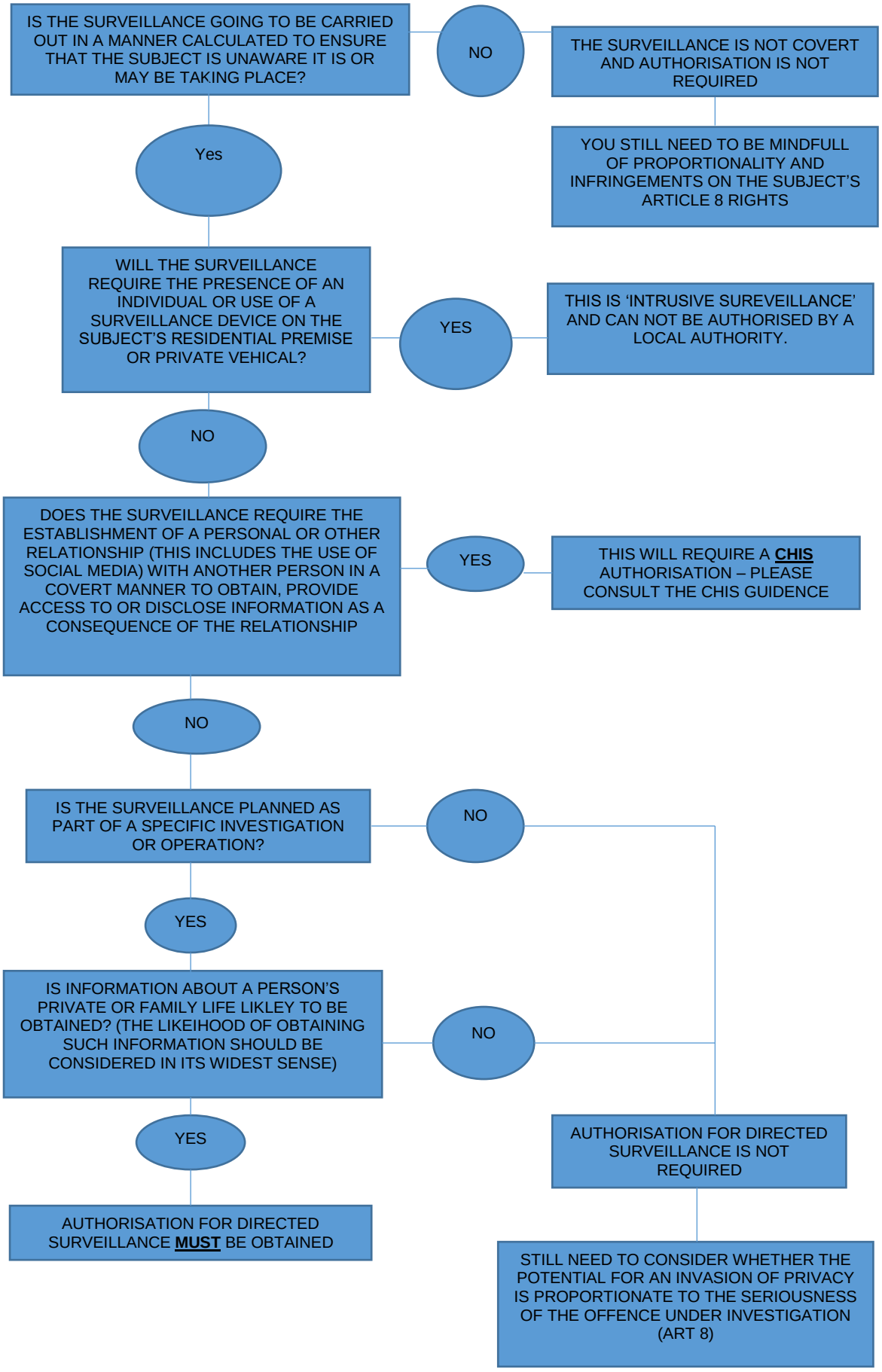
19.6 When informing a person of a Serious Error, the Commissioner must inform the person of any rights that they may have to apply to the Investigatory Powers Tribunal and provide such details of the error as the Commission considers to be necessary for the exercise of these rights.

19.7 Evidence gathered where RIPA has not been complied with may not be admissible in Court. Any perceived breach of this policy or the RIPA procedures should be reported to the Monitoring Officer. Where the breach relates to an active court case this should also be raised with the Solicitor instructed in this case. These should be reported as soon as they come to light.

20. **OTHER SOURCES OF ADVICE**

20.1 Detailed guidance on the operation of RIPA is available in Codes of Practice published by the Home Office and available on their website **www.homeoffice.gov.uk**. Advice is also available from the RIPA Monitoring Officer and Legal Services.

IS A DIRECTED SURVEILLANCE AUTHORISATION REQUIRED?



APPENDIX A

GUIDANCE TO STAFF ON USE OF COVERT HUMAN INTELLIGENCE SOURCES

This Guidance **must** be read in conjunction with the City of Lincoln Council's Policy on Regulation of Investigatory Powers Act 2000 (RIPA)

1. GENERAL POLICY

1.1 Please refer to the policy on RIPA for an explanation of the Regulation of Investigatory Powers Act 2000 and how this affects the Council.

1.2 The procedure and guidance set out in this Guidance is based on the provisions of RIPA, the Home Office Codes of Practice on the use of CHIS and the Home Office Guidance to Local Authorities in England and Wales on the Judicial Approved Process for RIPA and the Crime Threshold for Directed Surveillance. When implementing any procedure or policy contained within this guidance the officer and the Authorising Officer must ensure that there is compliance with the Home Office Codes of Practice on CHIS. This can be found at:

https://www.gov.uk/government/publications/covert-surveillance-and-covert-human-intelligence-sources-codes-of-practice

1.3 There is a Flowchart at the end of this Policy to summarise the requirements of RIPA.

1.4 To be clear, there is no use of a CHIS merely because a person offers information to the Council that may be material to the investigation of an offence, but there would be if the authority asks that person to obtain further information. If a person has a relationship with another person which is not established or maintained for a covert purpose, the fact that he or she does in fact covertly disclose information to the local authority will not require an authorisation and that person will not be a CHIS.

1.5 It is not only a person outside of the employment of the Council who may be used as a source. If a member of staff is intended to be used as a CHIS, appropriate training must be given to that staff member.

2. COVERT HUMAN INTELLIGENCE SOURCES

2.1 A person is a "covert human intelligence source" (CHIS) if:

1. They establish or maintain a personal or other relationship with a person for the covert purpose of facilitating the doing of anything falling within 2) or 3)
2. They covertly use such a relationship to obtain information or to provide access to any information to another person; or
3. They covertly disclose information obtained by the use of such a relationship or as a consequence of the existence of such a relationship

2.2 In this context, a source of information acts covertly if he or she establishes and maintains a relationship which is conducted in a manner which is calculated to ensure that the other person is unaware that the relationship is being used for the purposes listed above.

2.3 A relationship that is used covertly, and the information obtained is disclosed covertly, if and only if the relationship is used or the information is disclosed in a manner that is calculated to ensure that one of the parties to the relationship is unaware of the use or disclosure in question. Where a person acting in their role for the Council is intending to engage with members of the public online without disclosing their identity or purpose, a CHIS authorisation may be needed and the Council's RIPA Policy should be consulted and the Social Media Access form should be used.

2.4 When applied to a relationship "established" means "set-up." It does not require, as "maintains" does, endurance over any particular period. Repetition is not always necessary to give rise to a relationship but whether or not a relationship exists depends on all the circumstances including the length of time of the relationship and the nature of any covert activity.

2.5 The use of a CHIS involves inducing, asking or assisting a person to engage in the conduct of a CHIS or to obtain information by means of the conduct of such a CHIS.

2.6 RIPA regulates the "conduct and use" of covert human intelligence sources. An officer therefore requires authority both to act as a CHIS in person and to use anyone else (e.g. a member of the public or private investigator) as a CHIS.

2.7 Officers should carefully consider whether any potential human source of information might be a CHIS and if so to secure the necessary authority in accordance with this guidance and accompanying documents. It is worth noting that a person meets the CHIS criteria even if they volunteer information to an officer. Officers should ensure that they are familiar with the Home Office Code of Practice on the use of Covert Human Intelligence Sources and also seek advice from Legal Services if necessary.

2.8 There are separate forms to be completed for the use of a CHIS and for reviewing, renewing and cancelling the use of a CHIS. These need to be completed by the officer and signed by the Authorising Officer. These forms and guidance on them can be here:

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

https://www.gov.uk/government/publications/reviewing-the-use-of-covert-human-intelligence-sources-chis

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

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

3. AUTHORISING THE USE OF A CHIS

3.1 The need to make use of a CHIS is likely to be even more infrequent than for Direct Surveillance. It involves additional considerations and procedures. Authority to authorise the conduct or use of a CHIS can only be granted by the Authorising Officer as outlined in the Policy. The Council has resolved that this must be in conjunction with the RIPA Monitoring Officer.

3.2 Before authorising the conduct or use of a CHIS the Authorising Officer will not only need to take into account the general considerations as outlined in the main guidance on RIPA but will also need to be satisfied that the appropriate arrangements are in place for:

- The management and oversight of a CHIS by a designated officer who will also have responsibility for the CHIS's security and welfare
- Record keeping
- Ensuring that any records disclosing the identity of the CHIS are only made available on a strict "need to know" basis.

3.3 Vulnerable individuals and juveniles should only be used as sources in the most exceptional circumstances and special rules apply in these cases. Only the Chief Executive may authorise use of a juvenile or vulnerable CHIS.

"Vulnerable individuals" are defined as people in need of community care services by reason of physical, mental or other disability, age or illness and who are unable to take care of themselves or protect themselves against significant harm or exploitation.

"Juveniles" are persons under 18 years of age. Special safeguarding rules apply to the use or conduct of juveniles as sources. Under no circumstance should the use or conduct of a CHIS under 16 be authorised to give information on their parents or any person who has parental responsibility for them. Any authorisation for the use or conduct of a juvenile CHIS will only be for 1 month's duration as opposed to 12 months for all other CHIS.

Those authorised to grant the use of CHIS's will be extremely reluctant to issue authorisations for the use of vulnerable individuals or juveniles.

Where a CHIS is under the age of 16 years old the Council must ensure that an appropriate adult is present at all meetings between the juvenile source and any person representing the investigating authority.

3.4 Before authorising the use or conduct of a source, the Authorising Officer should take into account the risk of interference with the private and family life of persons who are not the intended subjects of the CHIS activity. This is known as Collateral Intrusion, a definition of Collateral Intrusion can be found in the RIPA Guidance above.

3.5 Measures should be taken, wherever practicable, to avoid or minimize interference with private and family life of those who are not the intended subjects of the CHIS activity. Where Collateral Intrusion is unavoidable, the activities may still be authorised providing this Collateral Intrusion is considered proportionate to the aims of the intended intrusion. Any Collateral Intrusion should be kept to the minimum necessary to achieve the objectives of the operation. All applications should include an assessment of the risk of any Collateral Intrusion and detail the measures taken to limit this to enable the Authorising Officer to properly consider the proportionality of the operation in light of the Collateral Intrusion.

3.6 The Authorising Officer who grants an authorisation should, where possible, be responsible for considering subsequent renewals of the Authorisation and any relevant security and welfare issues. The Authorising Officer will stipulate the frequency of formal reviews and The Controller should maintain an audit of case work sufficient to ensure that the use or conduct of the CHIS remains within the parameters of the Authorisation. This does not prevent additional reviews being conducted in response to the changing circumstances of an operation.

3.7 In some cases a single Authorisation my cover more than one CHIS. However it is only likely to be appropriate in situations where the activities to be authorised, the subjects of the operation, the interference with the private and family life, the likely Collateral Intrusion and the environmental or operational risk assessments are the same.

3.8 As of 1st November 2012 the Council now has to obtain an order from a Justice of the Peace (JP) approving the grant or renewal of any Authorisation for the use of CHIS before Authorisation can take affect and the operation be carried out. This is similar to the procedure outlined in the RIPA Policy and Legal Services advice is required to undertake this application.

The JP will consider whether or not the Authorisation for the use of a CHIS was necessary and proportionate. They will need to be satisfied that at the time the authorisation was granted or renewed or notice was given or renewed there was reasonable grounds for believing that the Authorisation or notice was necessary and proportionate. If the Justice of the Peace is satisfied that the statutory tests have been met and that the use of a CHIS is necessary and proportionate they will issue an order approving the grant or renewal of Authorisation as described in the application.

3.9 Authorisation for an adult CHIS (unless renewed) is for 12 months from the date of approval by the JP.

3.10 Regular reviews of the authorisations should be undertaken by the Authorising Officer to assess whether it remains necessary and proportionate to use a CHIS and whether the authorisation remains justified. The review should include:

- The use made of the CHIS during the period authorised
- The tasks given to the CHIS
- The information obtained from the CHIS

- If appropriate to the Authorising Officer's remit, the reasons why executive action is not possible at this stage.

Results of the review must be retained for at least 5 years. In each case it is up to the Authorising Officer to determine the frequency of a review. This should be as often as is considered necessary and proportionate but should not prevent reviews being conducted in response to changing circumstances. Where there are any significant or substantive changes to the nature of the operation, consideration should be given as to whether it is necessary to apply for a new authorisation.

3.11 CHIS authorisations can be renewed on more than one accession if necessary and provided that they continue to meet the criteria for authorisation. All renewals are subject to authorisation from a Justice of the Peace.

4. Necessity and Proportionality

4.1 The Act requires that the Authorising Officer (and then the JP) must believe that an Authorisation for the use or conduct of a CHIS is necessary and proportionate in the circumstances of the particular case for the purpose of preventing or detecting crime or of preventing disorder.

4.2 If it decides that the use of a CHIS is necessary the person granting the authorisation must then believe that the use is proportionate to what is sought to be achieved by the conduct and use of that CHIS. This involves balancing the intrusiveness of that CHIS on the target and others who might be affected by it against the need for the CHIS to be used in investigative and operational terms.

4.3 The use of a CHIS will not be proportionate if it is excessive in the circumstances of the case. Each action authorised should bring an expected benefit to the investigation or operation and should not be disproportionate or arbitrary. No activity will be considered proportionate if the information which is sought could reasonably be obtained by other less intrusive means.

4.4 When considering this the following factors are relevant:-

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

Fundamentally the use of covert surveillance must be proportional to the issue being investigated

The test for necessary needs to include a consideration of why it is necessary to use covert surveillance

4.5 The use of a CHIS should be carefully managed to meet the objective in question and sources must not be used in an arbitrary or unfair way.

5. Special Considerations for authorisation

5.1 Care should be taken in cases where the subject might reasonably expect a high level of privacy or where Confidential Information is involved. Please refer to the RIPA Policy for more detailed guidance on Confidential Information. Confidential Information could be legally privileged information, or information which carries medical or journalistic confidentiality. In cases where legally privileged material or other Confidential Information might be acquired the use or conduct of a CHIS can only be authorised by the Authorising Officer.

6. Officers Required

6.1 Two officers are required for the management of a CHIS: The Handler who has day-to-day responsibility and will be the contact for receipt of information, and The Controller who has general oversight.

6.2 Tasking the CHIS is the responsibility of The Handler with reference to The Controller. It is important to ensure that Authorisation is not drawn up so narrowly that new authorisation must be sought each time the CHIS is tasked however it can be difficult to predict the needs of an operation at the time of Authorisation and where an operation changes officers must ensure that the existing Authorisation is sufficient. Where it is not it should be cancelled and new Authorisation should be sought.

6.3 The Handler will have the day to day responsibility for:

- Dealing with a CHIS on behalf of the authority concerned
- Directing the day to day activities of the CHIS
- Recording the information supplied by the CHIS
- Monitoring the CHIS's security and welfare.

6.4 The Controller will be responsible for the management and supervision of the Handler and the general use and oversight of the CHIS.

6.5 Where the authorisation is for the use or conduct of a CHIS whose activities benefit more than a single public authority, responsibilities for the management and oversight of that CHIS may be taken up by one authority or can be split between the authorities. The Controller and Handler of a CHIS need not be from the same authority. The public authorities involved must lay out in writing their agreed oversight arrangements.

7. Keeping Records

7.1 Record keeping must be in accordance with The Regulation of Investigatory Powers (Source Records) Regulation S.I 2000; No 2725. Relevant officers will have their attention drawn to those specific requirements whenever an authorisation is issued

and specific advice given as to how they should be complied with in the circumstances of the case. Consideration should be given to the management of any requirement to disclose information tending to reveal the existence or identity of a CHIS to or in court.

7.2 A centrally retrievable record of all authorisations should be maintained. These records need only contain the name, code name, or unique identifying reference of the CHIS, the date the Authorisation was granted, renewal or cancellation and an indication as to whether the activities were self-authorised. These records should be made available to the relevant Commissioner or Inspector from the Office of Surveillance Commissioners upon request.

7.3 These records should be retained for a period of at least five years from the ending of the authorisation to which they relate. In retaining records consideration must be given to the duty of care owed to the CHIS, the likelihood of future criminal or civil proceedings relating to information supplied by the CHIS or activities undertaken and the responsibilities and obligations under the General Data Protection Regulations. All records kept should be maintained in such a way so as to preserve the confidentiality and prevent disclosure of the identity of the CHIS and the information provided by the CHIS.

7.4 Records or copies of the following, as appropriate, should be kept for at least five years:

- A copy of the authorisation together with any supplementary documentation and notification of the approval given by the Authorising Officer
- A copy of any renewal of an Authorisation, together with the supporting documentation submitted when the renewal was requested
- The reason / reasons why the person renewing an Authorisation considered it necessary to do so.
- Any risk assessment made in relation to a CHIS
- The circumstances in which tasks were given to the CHIS
- A record of the results of any reviews of the Authorisation
- The reasons, if any, for not renewing the Authorisation
- The reasons for cancelling an Authorisation
- The date and time when any instruction was given by the Authorising Officer that the conduct or use of a CHIS must cease
- A copy of the decision by an Ordinary Commissioner on the renewal of an authorisation beyond 12 months.

7.5 There must be arrangements in place for the secure handling, storage and destruction of material obtained through the use or conduct of a CHIS. This will be is done in compliance with the General Data Protection Regulations and the Council's policies.

8. **Security and Welfare**

8.1 Before authorising the use or conduct of a CHIS the Authorising Officer must ensure that a risk assessment is carried out to determine the risk to the CHIS of any tasking

and the likely consequences should the role of the CHIS become known. The ongoing security and welfare of the CHIS most be considered once the operation has terminated. This is to be carried out by the Corporate Health and Safety team.

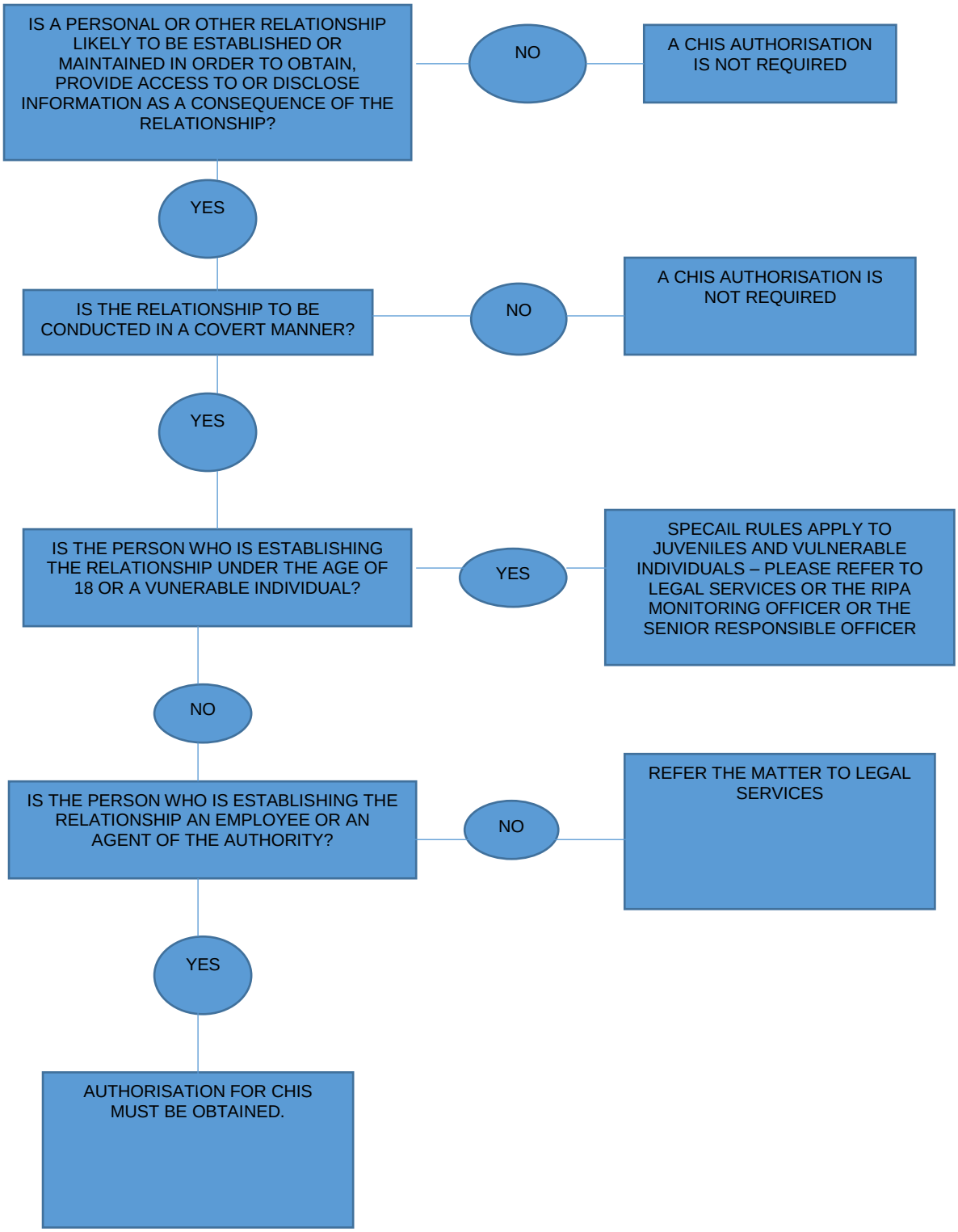
8.2 The Handler is responsible for bringing to the attention of the CHIS Controller any concerns about the personal circumstances of the CHIS insofar as this might affect:

- The validity of the risk assessment
- The conduct of the CHIS
- The safety and welfare of the CHIS

Where appropriate, concerns about such matters must be brought to the attention of the Authorising Officer and a decision must then be taken on whether or not to allow the Authorisation to continue.

8.3 The Council recognises a duty of care to its covert sources and it is importance that a risk assessment and management approach is taken with regard to the welfare of the source. The risk to the source may not only be physical but also psychological, for example stress.

IS A CHIS AUTHORISATION REQUIRED?



APPENDIX B

REQUEST TO ACCESS SOCIAL MEDIA FOR INVESTIGATIVE PURPOSES

FOR GUIDENCE FILLING OUT THIS FORM PLEASE REFER TO THE RIPA SOCIAL MEDIA GUIFDENCE ON NETCONSENT.

Social Media are "*websites and applications which enable users to create and share content or to participate in Social Networking"* For the avoidance of doubt this includes social networking sites.

THIS FORM ONLY ALLOWS YOU TO ACESS SOCIAL MEDIA SITES VIA COMMUNICATIONS, IT DOES NOT GIVE YOU AUTHORITY TO ACCESS THEM THOUGH YOUR OWN PERSONAL ACCOUNTS OR PERSONAL DEVICES.

LEAD OFFICER ……

SERVICE MANAGER …….

WHICH SOCIAL MEDIA / NETWORKING SITE DO YOU WISH TO ACCESS?

……
……

DOES THE TARGET HAVE PRIVACY SETTINGS APPLIED ON THESE SITES? Y / N / UNKNOWN

NATURE AND PURPOSE OF INVESTIGATION:

……
……
……
……
……
……
……
……

IF YOU ARE INVESTIGATING AN OFFENCE DOES THE OFFENCE CARRY A 6 MONTH CUSTODIAL SENTENCE OR LONGER IF THE SUSPECT IS CONVICTED? Y / N

IF YES, WHAT IS THE MAXIMUM CONVICTION FOR THE OFFENCE?

……

WHAT INFORMATION DO YOU HOPE TO FIND ON THE SITE?

……
……
……
……
……

…….....
.....

IT MUST BE PROPORTIONATE TO BREACH AN INDIVIDUAL'S ARTICLE 8 RIGHT, PLEASE EXPLAIN WHY YOU CONSIDER THIS BREACH TO BE PROPORTIONATE FOR THE PURPOSES OF THIS INVESTIGATION:

……
……
……
……
……
……
……
……

OUTLINE THE RISK (IF ANY) OF COLLATERAL INTRUSION?

……
……
……
……
……
……
……
……

COMMENTS FROM LEGAL SERVICES

……
……
……
……
……
……
……
……

SOLICITOR……..

DATE …….

PLEASE RETAIN A SIGNED COPY OF THIS FORM FOR YOUR FILE. COMMUNICATIONS WILL ALSO RETAIN A COPY OF THIS FORM.

ONCE THIS FORM HAS BEEN SIGNED BY LEGAL SERVICES IT WILL ENTITLE YOU TO VIEW A SUSPECTS SOCIAL MEDIA PAGE OR SOCIAL NETWORKING PAGE ONCE (VIA COMMUNICATIONS) AND RECORD YOUR FINDINGS.

SHOULD THE CASE GO TO COURT YOU MAY NEED TO VISIT THE SOCIAL MEDIA / SOCIAL NETWORK SITE AGAIN TO UPDATE YOUR FINDINGS, THIS FORM AUTHOMATICALLY ENTITLES YOU TO ACCESS THE SAME SOCIAL MEDIA OR SOCIAL NETWORKING SITED ONCE MORE PRIOR TO COURT IN ORDER TO UPDATE YOUR INFORMATION AND GIVE THE COURT CURRENT DETAILS. THE SITE CAN ONLY BE ACCESSED A SECOND TIME FOR THE PURPOSES OF A COURT HEARING AND YOU MUST ACCESS THE SOCIAL MEDIA / SOCIAL NETWORKING SITES THOUGH COMMUNICATIONS.

IF YOU NEED TO ACCESS THIS SITE MORE THAN TWICE THIS COULD BE DIRECTED SURVEILLANCE AND YOU WILL NEED TO SPEAK TO A MEMBER OF LEGAL SERVICES AS YOU MAY REQUIRE RIPA AUTHORISATION FROM THE COURTS BEFORE YOU CAN DO THIS.

I CONFIRM I HAVE READ AND UNDERSTOOD THE ABOVE

……..

DATE

……..