CORPORATE POLICY & PROCEDURES DOCUMENT

ON

THE REGULATION OF INVESTIGATORY POWERS ACT 2000 (RIPA)

Version No: 8
Last Revised: February 2018
Next Review: February 2019

CONTENTS PAGE **Page No.**

A	Introduction and Key Messages ……..…….	3
B	Senior Responsible Officer and Responsibilities.....	4
C	County Council Policy Statement ……..…..	4
D	Authorising Officer Responsibilities ……..……..	4
E	General Information on RIPA ……..……..	5
F	What RIPA Does and Does Not Do ……..……	7
G	Types of Surveillance ……..……..….	7
H	Conduct and Use of a Covert Human Intelligence Source (CHIS) ……	12
I	Acquisition of Communications Data…….	14
J	Authorisation Procedures …….	15
K	Application for Judicial Approval……..	18
L	Working with / through Other Agencies ……	21
M	Record Management ……..……..	22
N	Concluding Remark's…….…….	24

Appendix 1 -	List of Authorising Officer Posts	25
Appendix 2 -	RIPA Flow Chart	26
Appendix 3 -	RIPA A Forms: Directed Surveillance	27
Appendix 4 -	RIPA B Forms: Covert Human Intelligence Source (CHIS)	28
Appendix 5 -	Application for Judicial Approval for Authorisation	31

NB:
The Regulation of Investigatory Powers Act 2000 ('RIPA') refers to 'Designated Officers'. For ease of understanding and application within Lincolnshire County Council, this Corporate Policy & Procedures Document refers to 'Authorising Officers'. Furthermore, such officers can only act under RIPA if they have been duly "authorised" to do so. For the avoidance of doubt, therefore, all references to duly Authorising Officers refer to 'Designated Officers' under RIPA.

Acknowledgements:
a) The County Council is most grateful to Lord Colville of Culross and His Honour Jeremy Fordham, Assistant Commissioners of the Office of Surveillance Commissioners, for their instructive and helpful comments during their visits to the authority which have contributed to the development of this Corporate Policy & Procedures Document.

b) The County Council would also like to thank Birmingham City Council for its initial work in this area.

A. Introduction and Key Messages

1. **This Corporate Policy & Procedures Document is based upon the requirements of The Regulation of Investigatory Powers Act 2000 as amended ('RIPA') and the Home Office's Codes of Practice on Covert Surveillance, Covert Human Intelligence Sources and the Acquisition and Disclosure of Communications Data.**

2. **The authoritative position on RIPA is, of course, the Act itself and any Officer who is unsure about any aspect of this Document should contact, at the earliest possible opportunity, the County Council Legal Services Section for advice and guidance. Appropriate training will be provided or organised by Legal Services to Authorising Officers and any other appropriate persons.**

3. **To ensure easy access, a copy of this Document and related Forms will be placed on the intranet.**

4. **The Legal Services Section will maintain and check the Central Register of all surveillance and covert human intelligence sources RIPA authorisations, reviews, renewals, cancellations and rejections. A similar register in relation to the acquisition of communication data will be maintained by the Authority's designated SPOC. However, it is the responsibility of the relevant Authorising Officer to ensure that Legal Services receive a copy of the relevant form within 1 week of the authorisation, review, renewal, cancellation or rejection.**

5. **RIPA and this Document are important for the effective and efficient operation of the County Council's actions with regard to covert surveillance, Covert Human Intelligence Sources and the Acquisition of Communications Data. This Document will, therefore, be kept under annual review by Legal Services. Authorising Officers must bring any suggestions for continuous improvement of this Document to the attention of Legal Services at the earliest possible opportunity. An annual review of this policy will also be presented to elected members by the Senior Responsible Officer within the Corporate Management Team together with quarterly internal reports to the relevant elected members to ensure that the policy remains fit for purpose and is being implemented in accordance with the requirements of the policy.**

6. **In terms of monitoring e-mails and internet usage, it is important to recognise the important interplay and overlaps with the County Council's e-mail and internet policies, Codes of Practice, Guidance, the Data Protection Act 1998 (and its Code of Practice) and the Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000. RIPA forms should be used where relevant and they will be only relevant where the criteria listed on the Forms are fully met.**

7. **If you are in any doubt on RIPA, this Document or the related legislative provisions, please consult Legal Services at the earliest possible opportunity.**

B. County Council Policy Statement

1. **The County Council takes seriously its statutory responsibilities and will, at all times, act in accordance with the law and take necessary and proportionate action in these types of matters. In that regard, the Legal Services Section, will keep this Document up to date and amend, delete, add or substitute relevant provisions, as necessary.**

2. **In carrying out the key functions of the County Council RIPA will be used by officers of the County Council when undertaking any investigative function that involves the use of Directed Surveillance, Covert Human Intelligence Sources or the Acquisition of Communications Data.**

C. Senior Responsible Officers and Responsibilities

1. **For the purpose of surveillance and the use of covert human intelligence sources the Senior Responsible Officer will be a member of the Corporate Management Team and in addition to the duties set out below, the Senior Responsible Officer will undertake reports to the elected members in relation to this policy.**

2. **In relation to the acquisition of communications data the Senior Responsible Officer will be someone of suitable senior rank within the Corporate Management team who is also someone designated as an authorising officer for the purpose of acquisition of communications data. This person will be the Communications Senior Responsible Officer.**

3. **The Senior Responsible Officers will ensure the integrity of the processes in place in relation to the use of covert human intelligence sources, surveillance and the acquisition of communications data within the Authority and monitor compliance with the Act and any relevant codes of practice. They will also liaise with the relevant Inspectors when an inspection is undertaken and oversee the implementation of any post-inspection action plans.**

D. Authorising Officer Responsibilities

1. **This Corporate Policy and Procedures Document and the forms included within it, will become operative from 1st February 2006. Authorising officers must be properly trained in the relevant areas of authorisation and must be in a post of Director, Head of Service, Service Manager or equivalent. Within the Fire and Rescue Service an authorising officer must be of the rank of Group Manager. It is important therefore, that relevant Directors, Heads of Service and Authorising**

Officers take personal responsibility for the efficient and effective operation of this policy and procedure within their respective areas.

2. **It will be the responsibility of Authorising Officers who have been duly empowered to ensure their relevant members of staff are also suitably trained as 'Applicants' so as to avoid errors in the operation of the process and completion of the relevant forms.**

3. **Authorising Officers will also ensure that staff who report to them follow this Corporate Policy & Procedures Document and do not undertake or carry out any form of surveillance without first obtaining the relevant authorisations in compliance with this Document.**

4. **Authorising Officers must also pay particular attention to Health and Safety issues that may be raised by any proposed surveillance activity. Under no circumstances, should an Authorising Officer approve any RIPA form unless, and until s/he is satisfied the health and safety of Council employees/agents are suitably addressed and/or risks minimised, so far as is possible, and proportionate to/with the surveillance being proposed. If an Authorising Officer is in any doubt, s/he should obtain prior guidance on the same from his/her Chief Officer, the County Council's Health & Safety Officer and/or the Legal Services Section.**

5. **Authorising Officers must also ensure when sending copies of any Forms to colleagues, Legal Services (or any other relevant authority), that they are sent in sealed envelopes and marked 'RIPA - Strictly Private and Confidential'. Alternatively, they may be sent as attachments by password protected and confidential e-mail.**

E. General Information on RIPA

1. **The Human Rights Act 1998 (which brought much of the European Convention on Human Rights and Fundamental Freedom 1950 into UK domestic law) requires the County Council and organisations working on its behalf, pursuant to Article 8 of the European Convention, to respect the private and family life of a citizen, his home and his correspondence.**

2. **The European Convention did not, however, make this an absolute right, but a qualified right. Accordingly, in certain circumstances, the County Council may interfere in the citizen's right mentioned above, if such interference is:-**

   (a) in accordance with the law;

   (b) necessary (as defined in this Document); and

   (c) proportionate (as defined in this Document).

3. **The Regulation of Investigatory Powers Act 2000 ('RIPA') provides a statutory mechanism (i.e. 'in accordance with the law') for authorising covert surveillance, the use of a 'covert human intelligence source' ('CHIS') – e.g. undercover agents and the acquisition of communications data. It seeks to ensure that any interference with an individual's right under Article 8 of the European Convention is necessary and proportionate. In doing so, RIPA seeks to ensure that both the public interest and the human rights of individuals are suitably balanced.**

4. **Directly employed Council staff and external agencies working for the County Council are covered by the Act for the time they are working for the County Council. All external agencies must, therefore, comply with RIPA and the work carried out by agencies on the Council's behalf must be properly authorised by one of the Council's designated Authorising Officers. (Authorising Officers are those whose posts appear in Appendix 1 to this Document).**

5. **If the correct procedures are not followed, evidence may be disallowed by the courts, a complaint of maladministration could be made to the Ombudsman, and/or the Council could be ordered to pay compensation. Such action would not, of course, promote the good reputation of the County Council and will, undoubtedly, be the subject of adverse press and media interest. It is essential, therefore, that all involved with RIPA comply with this Document and any further guidance that may be issued, from time to time, by the Legal Services.**

6. **<u>NB:</u> It is important to note new changes to local authority powers – these were introduced by the Protection of Freedoms Act 2012 and the Regulation of Investigatory Powers (Directed Surveillance and Covert Human Intelligence Sources) (Amendment) Order 2010 (the 2012 Order). The impact of the changes is that local authorities can only authorise directed surveillance to prevent or detect criminal offences that:**

- **Are punishable with a term of six months imprisonment or more or**
- **Are related to the sale of tobacco or alcohol to underage persons**
- **In all cases where this authority wishes to use directed surveillance, acquisition of communications data or the use of a covert human intelligence source under RIPA the authority needs to obtain an order approving the grant or renewal of an authorisation from a justice of the peace or district judge at the Magistrates' Court before it can take effect.**
- **This new judicial approval is an additional stage in the process and the local authority process of applications to authorising officers on the appropriate forms applying the tests of proportionality and necessity in accordance with the code of practice still applies as set out in this policy document.**

A flowchart outlining the Local Authority Procedure: Application to a Justice of the Peace seeking an order to approve the grant of a RIPA authorisation or notice is included as Appendix 2

F. What RIPA Does and Does Not Do

1. RIPA does:

- **require prior authorisation of directed surveillance.**
- **prohibit the Council from carrying out intrusive surveillance.**
- **require authorisation of the conduct and use of a CHIS.**
- **require safeguards for the conduct and use of a CHIS.**
- **permit the Council to acquire communications data in certain circumstances.**

2. RIPA does not:

- **make unlawful conduct which is otherwise lawful.**

- **prejudice or dis-apply any existing powers available to the County Council to obtain information by any means not involving conduct that may be authorised under this Act. For example, it does not affect the County Council's current powers to obtain information via the DVLA or to get information from the Land Registry as to the ownership of a property.**

3. If the Authorising Officer or any Applicant is in any doubt, s/he should speak to a representative from the Legal Services section BEFORE authorising, renewing, cancelling or rejecting any directed surveillance, use of a CHIS and/or acquisition of communications data.

G. Types of Surveillance

1. 'Surveillance' includes

- **monitoring, observing, listening to persons, watching or following their movements, listening to their conversations and other such activities or communications.**

- **recording anything mentioned above in the course of authorised surveillance.**

- **surveillance, by or with, the assistance of appropriate surveillance device(s).**

Surveillance can be overt or covert.

2. ***Overt Surveillance***

Most of the surveillance carried out by the County Council will be done overtly – there will be nothing secretive, clandestine or hidden about it. In many cases, Officers will be behaving in the same way as a normal member of the public (e.g. in the case of most test purchases), and/or will be going about Council business openly (e.g. a market inspector walking through markets).

3. **Similarly, surveillance will be overt if the subject has been informed it will happen (e.g. where a noisemaker is warned (preferably in writing) that noise will be recorded if the noise continues, or where an entertainment licence is issued subject to conditions, and the licensee is told that officers may visit without notice or identifying themselves to the owner/proprietor to check that the conditions are being met.**

4. ***Covert Surveillance***

Covert Surveillance is carried out in a manner calculated to ensure that the person subject to the surveillance is unaware of it taking place. (Section 26(9) (a) of RIPA).

5. **RIPA regulates two types of covert surveillance, (Directed Surveillance and Intrusive Surveillance) and the use of Covert Human Intelligence Sources (CHIS's).**

6. ***Directed Surveillance***

Directed Surveillance is surveillance which:-

- **is covert; and**
- **is not intrusive surveillance (see definition below – the County Council must not carry out any intrusive surveillance);**
- **is not carried out in an immediate response to events which would otherwise make seeking authorisation under the Act unreasonable, e.g. spotting something suspicious and continuing to observe it; and**
- **it is undertaken for the purpose of a specific investigation or operation in a manner likely to obtain private information about an individual (whether or not that person is specifically targeted for purposes of an investigation). (*Section 26(10) of RIPA).***

7. ***Private information*** **in relation to a person includes any information relating to his private and family life, his home and his correspondence. The fact that covert surveillance occurs in a public place or on business premises does not mean that it cannot result in the obtaining of private information about a person. Prolonged surveillance targeted on a single person will undoubtedly result in the obtaining of**

private information about him/her and others that s/he comes into contact, or associates, with.

8. Similarly, although overt town centre CCTV cameras do not normally require authorisation, if the camera is tasked for a specific purpose, which involves prolonged surveillance on a particular person, authorisation will be required. The way a person runs his/her business may also reveal information about his or her private life and the private lives of others.

9. For the avoidance of doubt, only those Officers designated and certified to be 'Authorising Officers' for the purpose of RIPA can authorise 'Directed Surveillance' IF, AND ONLY IF, the RIPA authorisation procedures detailed in this Document, from 1st February 2006, are followed. If an Officer has not been "authorised" for the purposes of RIPA, s/he can NOT carry out or approve/reject any action set out in this Corporate Policy & Procedures Document.

10. *Intrusive Surveillance*

This is when it:-

- **is covert;**
- **relates to residential premises and private vehicles; and**
- **involves the presence of a person in the premises or in the vehicle or is carried out by a surveillance device in the premises/vehicle. Surveillance equipment mounted outside the premises will not be intrusive, unless the device consistently provides information of the same quality and detail as might be expected if they were in the premises/vehicle.**

11. This form of surveillance can be carried out only by police and other law enforcement agencies. County Council Officers must not carry out intrusive surveillance.

Surveillance of County Council Employees

12. As a public authority we are bound by Article 8 of the European Convention on Human Rights and cannot undertake any surveillance of an individual unless it falls within our core function as an authority and relates to the investigation of a criminal offence which attracts a custodial sentence of six months or more. Where an employee is suspected of involvement in activity that amounts to such a criminal offence then we have a function to protect the wellbeing of the people of Lincolnshire and where this impacts upon the resources of the County Council paid for out of public funds this clearly involves our powers under Section 1 of the Local Government Act 2000 to take appropriate action to protect the wellbeing of the area and the RIPA policy should be followed when any activity covered by it is being considered. Surveillance of employees is also governed by the Data

Protection Act and the Employment Practice Code and Supplemental Code published by the Information Commissioners Office. This emphasises that covert monitoring of employees should only take place in exceptional circumstances and should only be used for the prevention and detection of crime. Such activity should form part of a specific investigation and be strictly targeted used within a set time frame.

Covert surveillance of County Council employees may not be authorised under RIPA solely for employment/disciplinary investigations.

13. <u>Proportionality</u>

The term incorporates three concepts:

- **the means should not be excessive in relation to the gravity of the mischief being investigated;**
- **the least intrusive means of surveillance on the target and others should be chosen and that all available overt means have been considered and rejected; and**
- **collateral intrusion involves invasion of third parties privacy and should, so far as is possible, be minimised.**

When making an application for directed surveillance consider:

- **Is the matter a criminal offence carrying at least six months imprisonment or a relevant offence of sale of alcohol or tobacco to an underage person**
- **Have I balanced the size and scope of the proposed surveillance activity against the gravity and extent of the perceived crime or offence?**
- **Have I considered all alternative methods of obtaining the necessary result and am I satisfied that those methods would not produce the result I am seeking?**
- **Have I carefully considered all aspects of collateral intrusion and have I minimised the risk of such intrusion as far as possible?**
- **Does the risk of collateral intrusion outweigh the perceived need to carry out the surveillance?**
- **Have I evidenced all of the above in my application?**

REMEMBER: No activity should be considered proportionate if the information which is sought could reasonably be obtained by other less intrusive means. Extra care should also be taken over any publication of the product of the surveillance.

14. Further guidance on surveillance can be found in the Home Office's statutory Code of Practice for Covert Surveillance and Property Interference at

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

Examples of different types of Surveillance

Type of Surveillance	Examples
Overt	• **Police Officer or Parks Warden on patrol** • **Signposted Town Centre CCTV cameras (in normal use)** • **Recording noise coming from outside the premises after the occupier has been warned in writing that this will occur if the noise persists.** • **Most test purchases (where the officer behaves no differently from a normal member of the public).**
Covert but not requiring prior authorisation	• **CCTV cameras providing general traffic, crime or public safety information.**
Directed must be RIPA authorised	• **Officers follow an individual or individuals over a period, to establish whether s/he is working when claiming benefit or off long term sick from employment.** • **Test purchases where the officer has a hidden camera or other recording device to record information which might include information about the private life of a shop-owner, e.g. where s/he is suspected of running his business in an unlawful manner.**
Intrusive – County Council cannot do this!	• **Planting a listening or other device (bug) in a person's home or in their private vehicle.**

H. Conduct and Use of a Covert Human Intelligence Source (CHIS)

Who is a CHIS?

1. **Someone who establishes or maintains a personal or other relationship for the covert purpose of helping the covert use of the relationship to obtain information.**

2. **RIPA does not apply in circumstances where members of the public volunteer information to the County Council as part of their normal civic duties, or to contact numbers set up to receive information.**

What must be authorised?

3. **The Conduct or Use of a CHIS require prior authorisation.**

   - **Conduct of a CHIS = Establishing or maintaining a personal or other relationship with a person for the covert purpose of (or is incidental to) obtaining and passing on information.**

   - **Use of a CHIS = Actions inducing, asking or assisting a person to act as a CHIS and the decision to use a CHIS in the first place.**

4. **The Council can use CHIS's IF, AND ONLY IF, RIPA procedures, detailed in this Document are followed.**

Juvenile Sources

5. **Special safeguards apply to the use or conduct of juvenile sources (i.e. children under the age of 18). On no occasion can a child under 16 years of age be authorised to give information against his or her parents. Only the Chief Executive of the County Council is permitted to authorise the use of Juvenile Sources, as there are other onerous requirements for such matters. Authorisations in respect of Juvenile CHIS must not exceed 1 month.**

Vulnerable Individuals

6. **A Vulnerable Individual is a person who is or may be in need of community care services by reason of mental or other disability, age or illness and who is or may be unable to take care of himself or herself, or unable to protect himself or herself against significant harm or exploitation.**

7. **A Vulnerable Individual will only be authorised to act as a source in the most exceptional of circumstances. Only the Chief Executive of the County Council is permitted to authorise the use of vulnerable individuals, as there are other onerous requirements for such matters.**

Test Purchases

8. Carrying out test purchases will not generally (as highlighted above) require the purchaser to establish a relationship with the supplier with the covert purpose of obtaining information and, therefore, the purchaser will not normally be a CHIS. For example, authorisation would not normally be required for test purchases carried out in the ordinary course of business (e.g. walking into a shop and purchasing a product over the counter as or similar to an ordinary member of the public).

9. By contrast, developing a relationship with a person in the shop, to obtain information about the seller's suppliers of an illegal product (e.g. illegally imported products will require authorisation as a CHIS. Similarly, using mobile hidden recording devices or CCTV cameras to record what is going on in the shop will require authorisation as directed surveillance. A combined authorisation can be given for a CHIS and directed surveillance. However, both directed surveillance and CHIS application forms will need to be completed and authorisation obtained. The forms should also be cross referenced.

9A. Where there is a test purchase of sales to juveniles for such matters as underage sales of alcohol or tobacco it will not normally be necessary to obtain authorisation for a CHIS. However, if the same test purchaser is used for repeat purchases from the same premises consider whether this has been done in such a way as to encourage familiarity with the purchaser and thereby developing a relationship that may require CHIS authorisation. If the test purchaser is carrying recording equipment or the purchase is observed by an officer this would require authorisation as directed surveillance.

Anti-social behaviour activities (e.g. noise, violence, race etc)

10. Persons who complain about anti-social behaviour, and are asked to keep a diary, will not normally be a CHIS, as they are not required to establish or maintain a relationship for a covert purpose. Recording the level of noise (e.g. the decibel level) will not normally capture private information and, therefore, does not require authorisation.

11. The current advice from the OSC is that measuring levels of noise audible in the complainant's premises is not surveillance because the noise has been inflicted by the perpetrator who has probably forfeited any claim to privacy. However, using sensitive equipment to discern speech or other noises not discernible by the unaided ear is covert as you are likely to obtain private information and where this is being recorded from the perpetrator home is also intrusive surveillance which local authorities cannot and must not undertake. Thus, only equipment capable of recording the volume of the noise or that records only what could be heard from the location of the monitoring equipment if being monitored by the unaided ear should be used.

Further Information

Further guidance on CHIS's can be found in the Home Office's Use of Covert Human Intelligence Sources statutory Code of at:

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

I. Acquisition of Communications Data

What is Communications Data?

1. **Communication data means any traffic or any information that is or has been sent by over a telecommunications system or postal system, together with information about the use of the system made by any person.**

Procedure

2. **There are two powers granted by S22 RIPA in respect of the acquisition of Communications Data from telecommunications and postal companies ("Communications Companies").**

3. **S22 (3) provides that an authorised person can authorise another person within the same relevant public authority to collect the data. This allows the local authority to collect the communications data themselves, i.e. if a private telecommunications company is technically unable to collect the data, an authorisation under this section.**

4. **In order to compel a Communications Company to obtain and disclose, or just disclose Communications Data in their possession, a notice under S22 (4) RIPA must be issued. The sole grounds to permit the issuing of a S22 notice by a Permitted Local Authority is for the purposes of "preventing or detecting crime or of preventing disorder". The issuing of such a notice will be the more common of the two powers utilised, in that the Communications Company will most probably have means of collating and providing the communications data requested.**

5. **S22 (3) should only be used where the local authority is seeking to collect the information themselves, i.e. either to install its own monitoring system/equipment or to use its own staff to collect the information from the Communications Company's system, without using the Communication Company's own staff.**

6. **S22 (4) should be used when the Communications Company is being asked to collect the requested information themselves prior to disclosure.**

7. **Usage of S22 (4) will be the more common form, in that the majority of the Communications Companies will have sufficient resources in place to allow them to collect the information following the service of a Notice.**

8. **Once a notice has been issued, it must be sent to the Communications Company. In issuing a notice, the Authorising Officer can authorise another person to liaise with the Communications Company covered by the notice.**

9. **For Lincolnshire County Council authorising officers who have been duly authorised by the chief legal officer for the purposes of RIPA may sign the Forms. Copies of any Forms must, however, be provided to the Chief Legal Officer within 1 week of signing the form.**

10. The Authority uses the NAFN service to administer applications for accessing communications data. Applicants will complete the online application that will be reviewed by the NAFN single point of contact (SPOC). The SPOC will accept, reject or request amendments to the application as necessary. Once satisfied the SPOC will pass notify the Authorising Officer that the application is ready for review.

12. If the application is authorised NAFN will provide the Investigating Officer with completed forms to enable them to seek Judicial Approval.

13. Once approval has been granted a copy of the signed approval should be sent to the SPOC who will serve the appropriate notice.

J. Authorisation Procedures

1. Directed surveillance and the use of a CHIS can only be lawfully carried out if properly authorised, and in strict accordance with the terms of the authorisation. A flowchart outlining the Local Authority Procedure: Application to a Justice of the Peace seeking an order to approve the grant of a RIPA authorisation or notice is included as Appendix 2. All authorisations and renewals for surveillance or CHIS must be in writing and subject to judicial approval before any activity for which authorisation is being sort can be commenced regardless of its urgency.

Authorising Officers

2. Forms can only be signed by Authorising Officers, authorised to do so by the County Solicitor. Authorised posts are listed in Appendix 1. This Appendix will be kept up to date by Legal Services, and added to as needs require. If a Chief Officer wishes to add, delete or substitute a post, s/he must refer such request to Legal Services for consideration, as necessary. Legal Services has been duly authorised to add, delete or substitute posts listed in Appendix 1.

3. Authorisations under RIPA are separate from delegated authority to act under the Council's Scheme of Delegation and internal departmental Schemes of Management. RIPA authorisations are for specific investigations only, and must be renewed or cancelled once the specific surveillance is complete or about to expire. The authorisations do not lapse with time! Authorisations to collect communications data under S22 (3) have, as with Section 22 (4) Notices a life span of one month. However, they can be renewed by serving a new authorisation or notice for further months, within the current life of the notice.

Training Records

4. Proper training will be given, or approved by Legal Services before Authorising Officers are permitted to sign any RIPA Forms. A Central Register of all those individuals who have undergone training will be kept by Legal Services.

Application Forms

6. Only the approved RIPA forms set out in this Document must be used. Any other forms used, after 1st February 2006, will be rejected by the Authorising Officer and/or Legal Services.

To comply with the duty to consider collateral intrusion properly the applicant and the authorising of6A. BEST PRACTICE FOR APPLICATIONS AND AUTHROISATION

- **When making an application for any covert activity or considering whether you need to make the same avoid labelling your activity such as "test purchase" as each activity should be judged on its specific facts and you need to consider each time what you are actually doing and whether there is a potential to meet the criterion for surveillance or CHIS. Avoid labels or a one size fits all approach as this can result in overlooking that what you actually doing.**
- **Do not create templates or cut and paste when completing an application but carefully consider each criteria afresh and complete a unique application for the authorisation you seek**
- **Be explicit about what you are seeking authorisation for and name any specific targets setting out clearly when, where and in what circumstances you are seeking the surveillance of a named target.**
- **Authorisations should also be explicit in terms of what is being authorised including what activity and equipment is being used.**
- **The authorising officer should set out in his/her won wards why he/she is satisfied or believes that he activity is necessary and proportionate using wording such as "I believe" or "I am satisfied".**
- **Included in the application should be a clear outline of the value of the information or intelligence that seeking to obtain.**
- **Where something is added to the authorisation which was not included in the application these additions should be carefully noted and explained as to why it is being added and equally where something applied for is not included in the authorisation its exclusion should also be explained.**
- **Cancellations should take place as soon as possible and the information on cancellation should include the time, date and reason for cancellation and confirm that any surveillance equipment has been removed and returned to storage.**
- **You should also at the point of cancellation record the value of the surveillance/information obtained during the authorisation period.**
- **Anything added by the authorising officer to the application should be hand written and signed by hand to avoid any suggestion that someone else has authorised it and it has just been signed off by the authorising officer.**

6B. RECORDING EQUIPMENT – Both the applicant and the authorising officer should understand the capacity of any recording equipment being used and where it is being deployed to be able to accurately assess the collateral intrusion likely to be occasioned by that equipment and ensure its use remains proportionate. Where equipment automatically records that which is outside the scope of what is needed by the authorisation in terms of necessity and/or proportionality will not of itself automatically

negate authorisation provided any such additional data is reviewed by the authorising officer and data which exceeds the parameters of the surveillance should be immediately disposed of.

7. ‘A Forms’ (Directed Surveillance)

Form	**A 1**	**Application for Authority for Directed Surveillance**
Form	**A 2**	**Review of Directed Surveillance Authority**
Form	**A 3**	**Cancellation of Directed Surveillance Authority**
Form	**A 4**	**Renewal of Directed Surveillance**
Appendix 5		**Application/Order for Judicial Approval**

8. ‘B Forms’ (CHIS) – See Appendix 4

Form	**B 1**	**Application for Authority for Conduct and Use of a CHIS**
Form	**B 2**	**Review of Conduct and Use of a CHIS**
Form	**B 3**	**Cancellation of Conduct and Use of a CHIS**
Form	**B 4**	**Renewal of Conduct and Use of a CHIS**
Appendix 5		**Application/Order for Judicial Approval**

9. (Acquisition of Communications Data)

Applications must be made via the NAFN website. Forms will be generated and supplied by NAFN.

Grounds for Authorisation

10. Directed Surveillance (A Forms), the Conduct and Use of a CHIS (B Forms) and/or the acquisition of communications data, can only be authorised by the County Council: ‘For the prevention or detection of crime or of preventing disorder’ and not any of the other grounds specified in Sections 22(1), 28(3) or 29(3) of the Act.

Assessing the Application Form

11. Before an Authorising Officer signs a Form, s/he must:-

(a) Be mindful of this Corporate Policy & Procedures Document, the Training provided by the County Solicitor and any other guidance issued, from time to time, by the County Solicitor on such matters;

(b) Satisfy his/herself that the RIPA authorisation is:-

(i) in accordance with the law;
(ii) necessary for the prevention and detection of crime as stated in paragraph 10 above; and
(iii) proportionate to what it seeks to achieve.

(c) **In assessing whether or not the proposed surveillance is proportionate consider:**

- **the balance of the size and scope of the proposed activity against the gravity and extent of the perceived crime or offence.**
- **Does the application adequately explain why the method to be adopted will cause the least possible intrusion on the subject and others?**
- **Does the application show that the applicant has considered all alternative methods of obtaining the result and evidenced why these methods have not been implemented?**
- **Is the activity an appropriate use of the legislation and a reasonable way, having considered all reasonable alternative methods of obtaining the necessary result?**

REMEMBER: No activity should be considered proportionate if the information which is sought could reasonably be obtained by other less intrusive means.

<u>The least intrusive method will be considered proportionate by the courts.</u>

(d) Take into account the risk of intrusion into the privacy of persons other than the specified subject of the surveillance (Collateral Intrusion). Measures must be taken wherever practicable to avoid or minimise (so far as is possible) collateral intrusion and the matter may be an aspect of determining proportionality;

(e) Set a date for review of the authorisation and review on that date or as close to it as is practically possible;

(f) Allocate a Unique Reference Number (URN) for the application as follows:-

Department/Whether Directed Surveillance (DS), Covert Human Intelligence Source (CHIS) or Acquisition of Communications Data (ACD)/Year/Number of Application

e.g. TS/DS/06/01, TS/CHIS/06/01 or TS/ACD/06/01

(g) Ensure that any RIPA Departmental Register is duly completed, and that a copy of the RIPA Forms (and any review/cancellation of the same) is forwarded to the RIPA Co-ordinating Officer for inclusion in the RIPA Central Register, within 1 week of the relevant authorisation, review, renewal, cancellation or rejection. In the case of notices compelling the disclosure of communications data, a copy of the notice must be attached to the authorisation form.

<u>Additional safeguards when Authorising a CHIS</u>

12. When authorising the conduct or use of a CHIS, the Authorising Officer must also:-

(a) be satisfied that the conduct and/or use of the CHIS is <u>proportionate</u> to what is sought to be achieved;

(b) be satisfied that appropriate arrangements are in place for the management and oversight of the CHIS and this must address health and safety issues through a risk assessment;

(c) consider the likely degree of intrusion of all those potentially affected;

(d) consider any adverse impact on community confidence that may result from the use or conduct or the information obtained; and

(d) **ensure records contain particulars and are not available except on a need to know basis.**

K. Application for Judicial Approval

<u>NB:</u> The Home Office issued guidance in October 2012 to local authorities concerning the changes to RIPA introduced by the Protection of Freedom Act 2012 and similar guidance was also issued for Magistrates' Courts. Officers considering an application for Judicial Approval of a RIPA authorisation are advised to consider both sets of guidance to assist in assessing whether their application to the court meets the criteria contained in the guidance as incomplete and/or inappropriate applications harm the reputation of the Council and waste resources.

All RIPA authorisations whether they are for direct surveillance, CHIS or communications data require judicial approval.

Before making an application for Judicial Approval of a RIPA authorisation the applicant officer and the authorising officer should consider again that:

- **In the case of an application relating to directed surveillance the case meets the criminal threshold and involves the investigation of a criminal offence that has a statutory sentence of at least six months imprisonment or involves the sale of alcohol or tobacco to a person under the age of 18 years.**

.

- **In the case of an application for a CHIS or communications data the case involves it is for the purpose of detecting or preventing crime or preventing disorder.**

- **The authorisation is necessary**

- **The authorisation is proportionate**

- **The person granting the authorisation is an appropriate person in terms of their rank and designation within the Council**

- **The information relied on to make the application in the internal application for authorisation and the internal authorisation and all supporting paperwork on its own makes out the case for judicial approval of the RIPA authorisation It is NOT sufficient for an officer to provide oral evidence to the court of the information relied upon and if the information required by the court as to whether the authorisation meets the test for approval is not apparent from the paperwork then the court WILL refuse the application for approval'**

<u>Making the Application:</u>

The officer seeking judicial approval of a RIPA authorisation will need to contact the administrative office at the Magistrates' Court. In Lincolnshire all administrative matters are dealt with centrally at Lincoln Magistrates' Court and the court will only deal with applications for a hearing by way of request by email.

When requesting a hearing of the application for judicial approval it should be made clear what the application is for and that what is sought is a hearing before a single lay magistrate or the district judge in private. This would usually take place in a retiring room.

An appointment will be arranged for the hearing by the court and the court should be asked whether the papers should be sent in advance of the hearing or a set handed over on the day of the hearing. In any event a spare set should be taken to court on the day of the hearing in case paperwork has been misplaced.

The paperwork should consist of:

- **the internal application for authorisation and any supporting paperwork,**
- **the internal authorisation**
- **The Application/Order for Judicial Approval (Form Annex 5) with the application part completed and the order section left blank for completion by the court.**

<u>Attending the Hearing</u>

Before you attend the hearing ensure you have all the required paperwork and copies of the same. Also you must ensure that you are a duly authorised Authorising Officer of the Council for the purpose of making the application for judicial approval and in terms of giving evidence on oath on behalf of the Council and that you have with you the means of proving the same to the satisfaction of the court.

Also ensure that the person attending to make the application is someone who is not only conversant with the case for which the RIPA authorisation is sought and who can answer questions about it but also someone who is able to answer questions in respect of the Council's RIPA policy and procedures. It is recommended that wherever possible the Authorising Officer attends court with the Applicant.

Ensure that you attend for the appointment in good time suitably attired for court and book in with the court ushers at their desk so they are aware you have arrived and

ascertain from them where the application is being heard and wait where you can easily be notified when the matter is to be called.

Both lay magistrates and the district judge are addressed as "Sir" or "Madam". Once called in you will be placed on oath on a religious text of your choice or asked to affirm on oath. The magistrate or judge will read the paperwork and ask of you any additional questions they may have.

<u>The Decision</u>

The Magistrate or District Judge will consider the application and will have to satisfy themselves that:

- **The application is necessary and proportionate**
- **For an application in respect of directed surveillance it meets the criminal threshold.**
- **For CHIS or communications data it is necessary for the purpose of the detection or prevention of crime or the prevention of disorder.**
- **In respect of an application for a CHIS, that suitable arrangements have been made in respect of the health and safety of the CHIS, someone has day-to-day responsibility for the CHIS, someone has oversight for the CHIS and all relevant records are being maintained.**
- **That the RIPA Authorisation has been granted by someone of appropriate rank and designation within the Council.**

The magistrate or district judge will record their decision on the order section of the Application/Order form giving their reasons and sign, date and time the same and then provide a copy to the Council.

Authorisation commences with Judicial Approval. For directed surveillance the authorisation remains in place for 3 months unless cancelled. CHIS authorisations remain in place for 1 year unless cancelled unless the CHIS is a juvenile in which case approval remains in place for 1 month.

<u>Renewals</u>

A renewal must be authorised before the original authorisation period has expired but any renewal will run from the time the original period ends. The renewal also requires Judicial Approval again by submitting the paperwork this time including the application for renewal and the internal authorisation for renewal together with a new Judicial Approval Application/Order Form.

The information above for booking a hearing will have to be followed and the officer should factor in when the court is sitting and ensure that whilst the application is made just before the authorisation is due to expire it is made in time to be heard by the court.

The same Application/Order form is used for the renewal and all the paperwork will have to be lodged setting out the renewal application in the same way as for the initial application above. Information should be included as to why an extension is needed and in particular the content and value of the information obtained so far.

BEST PRACTICE:

- **The OSC advise that the best person to make the application for prior approval to the magistrates' court is the authorising officer as only he can explain his though process in terms of the proportionality, necessity and collateral intrusion elements of the application.**
- **If someone other than the authorising officer makes the application any comment made by the court should be reported back promptly and a record of the comments made and the action taken to incorporate or address those comments.**
- **An authorisation does not take effect until it has been approved by and signed by the magistrate. The date and time of signature by the authorising officer and the magistrate should be accurately recorded and then used for the purpose of recoding expiry dates.**

L. Working With/Through Other Agencies

1. **When some other agency has been instructed <u>on behalf of the County Council</u> to undertake any action under RIPA, this Document 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. They must be made aware explicitly what they are authorised to do.**

2. **<u>When some other agency</u> (e.g. Police, Customs & Excise, and Inland Revenue etc):-**

   (a) **wish to use the County Council's <u>resources</u> (e.g. CCTV surveillance systems), that agency must use its own RIPA procedures <u>and</u>, before any Officer agrees to allow the County Council's resources to be used for the other agency's purposes, s/he <u>must obtain</u> a copy of that agency's RIPA form for the record (a copy of which must be passed to Legal Services for the RIPA Central Register) and/or relevant extracts from the same which are sufficient for the purposes of protecting the County Council and the use of its resources;**

   (b) **wish to use the County Council's <u>premises for their own</u> 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 County 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 other agency for the County Council's co-operation in the agent's RIPA operation. In such cases, however, the County Council's own RIPA forms should not be used as the County Council is only 'assisting' not being 'involved' in the RIPA**

activity of the external agency.

3. **In terms of 2(a), if the Police or other Agency wish to use County Council resources for <u>general</u> 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 <u>before</u> any County Council resources are made available for the proposed use. Copies of letters should be sent as soon as possible to Legal Services for retention.**

4. **<u>If in doubt, please consult with Legal Services at the earliest opportunity</u>.**

M. Record Management

1. The County Council must keep a detailed record of all authorisations, renewals, cancellations and rejections in Departments and a Central Register of all Authorisation Forms will be maintained and monitored by Legal Services.

2. <u>Records maintained in the Department</u>

The following documents must be retained by the relevant Chief Officer (or his/her designated departmental representative) for such purposes.

- **a copy of the Forms together 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 reviews prescribed by the Authorising Officer;**
- **a record of the result of each review of the authorisation;**
- **a copy of any renewal of an authorisation, together with the supporting documentation submitted when the renewal was requested;**
- **the date and time when any instruction was given by the Authorising Officer;**
- **the <u>Unique Reference Number</u> for the authorisation (URN).**

3. <u>Each</u> form will have a URN. The departmental representative will issue the relevant URN to Applicants. The cross-referencing of each URN takes place <u>within</u> the Forms for audit purposes. The relevant Departmental code to be followed is as per Appendix 1. Rejected Forms will also have URN's.

<u>Central Register maintained by Legal Services</u>

4. Authorising Officers must forward details of each Form to the RIPA Co-ordinating Officer for the Central Register, <u>within 1 week of the authorisation, review, renewal, cancellation or rejection</u>. Legal Services will monitor the same and give appropriate guidance, from time to time, or amend this Document, as necessary.

5. The County Council will retain the following records for a period of at least three years from the ending of the authorisation. The Office of the Surveillance Commissioners (OSC) can audit/review the County Council's policies and procedures, and individual authorisations.

:

- **The type of authorisation;**
- **The date the authorisation was given;**

- **Name rank/grade of the authorising officer;**
- **The unique reference number (URN) of the investigation or operation;**
- **The title of the investigation including a brief description and names of the subjects if known;**
- **If the authorisation has been renewed, when it was renewed and who authorised the renewal, including the name and rank/grade of the authorising officer;**
- **Whether the investigation or operation is likely to result in the obtaining of confidential information as defined in the code of practice;**
- **Whether the authorisation was granted by an individual directly involved in the investigation;**
- **The date the authorisation was cancelled.**

In relation to <u>directed surveillance authorisations</u> the following documentation should be centrally retrievable for a period of five years:

- **Copies of all applications, authorisations and any supplementary documentation and notifications of approval given by the authorising officer;**
- **Copies of Application/Order for Judicial Approval**
- **A record of the period over which surveillance has taken place**
- **The frequency of reviews prescribed by the authorising officer and a record of the result of each review;**
- **A copy of all renewal requests and authorisations together with supporting documentation**
- **The date and time when any instruction to cease surveillance was given.**
- **The date and time when any other instruction was given by the authorising officer.**

In relation to <u>CHIS authorisations</u> the following documentation should be centrally retrievable for a period of five years:

- **A copy of, applications, authorisations, notifications of approval and renewals together with any supporting documentation;**
- **Copies of Application/Order for Judicial Approval**
- **The 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 a CHIS**
- **The value of a CHIS to the investigatory authority;**
- **A record of the results of any reviews of the authorisation**
- **The reasons why, if any, for not renewing an authorisation**
- **The reason for cancellation of an authorisation and the date and time when any instruction to cease the conduct or use of a CHIS was given.**

In relation to the acquisition of communications data the following documentation should be centrally retrievable for a period of five years:

- **A copy of applications, authorisations and copies of notices and any supporting documentation.**
- **Copies of Application/Order for Judicial Approval**
- **Records of the withdrawal of authorisations and the cancellation of notices.**
- **Numbers of applications that were rejected by authorising officers**
- **Numbers of notices requiring disclosure of communications data under each subsections of Section 21(4) or a combination thereof.**
- **Number of authorisations for conduct to acquire communications data under each subsections of Section 21(4) or a combination thereof.**
- **Number of times an urgent notice or authorisation is granted orally requiring disclosure of communications data under each subsections of Section 21(4) or a combination thereof.**

N. Concluding Remarks of Legal Services

1. **Where there is an interference with the right to respect for private life and family guaranteed under Article 8 of the European Convention on Human Rights, and where there is no other source of lawful authority for the interference, or if it is held not to be necessary or proportionate to the circumstances, the consequences of not obtaining or following the correct authorisation procedure set out in RIPA and this Document, may be that the action (and the evidence obtained) will be held to be unlawful by the Courts pursuant to Section 6 of the Human Rights Act 1998.**

2. **Obtaining an authorisation under RIPA and following this policy, will therefore ensure that the action is carried out in accordance with the law and subject to stringent safeguards against abuse of anyone's human rights.**

3. **Authorising Officers will be suitably trained and they must exercise their minds every time they are asked to sign a Form. They must never sign or rubber stamp Form(s) without thinking about their personal and the County Council's responsibilities**

4. **Any boxes not needed on the Form(s) must be clearly marked as being 'NOT APPLICABLE', 'N/A' or a line put through the same. Great care must also be taken to ensure accurate information is used and is inserted in the correct boxes. Reasons for any refusal of an application must also be kept on the form and the form retained in accordance with the Council's Financial Procedures – FP3 Asset Management.**

5. **For further advice and assistance on RIPA, please contact Legal Services. Details are provided on the front of this Document.**

APPENDIX 1

List of Authorising Officer Posts

No.	Position	Dept. Identifier
1	CHIEF EXECUTIVE	CX
2	ENVIRONMENT AND ECONOMY	
3	ADULT SOCIAL CARE	
4	CHILDREN'S SERVICES	
4	COMMUNITY WELLBEING AND PUBLIC HEALTH	
5	FINANCE AND PUBLIC PROTECTION	
	Trading Standards	TS
	1. Business and Public Protection Manager x 2	TS - SM
	3. Head of Trading Standards – First Reserve AO	TS - HoS
	4. NAFN– Single Point of Contact (SPOC) for Authority	NAFN

List of Designated Posts

No.	Position	Designation
1	Executive Director for Environment & Economy	Senior Responsible Officer
2	Principal Lawyer, Education, Employment & Prosecutions Team	RIPA Coordinating Officer

IMPORTANT NOTES

A. Even if a post is identified in the above list the persons currently employed in such posts are not authorised to sign RIPA Forms (including a renewal or cancellation) unless s/he has been authorised by Legal Services to do so.

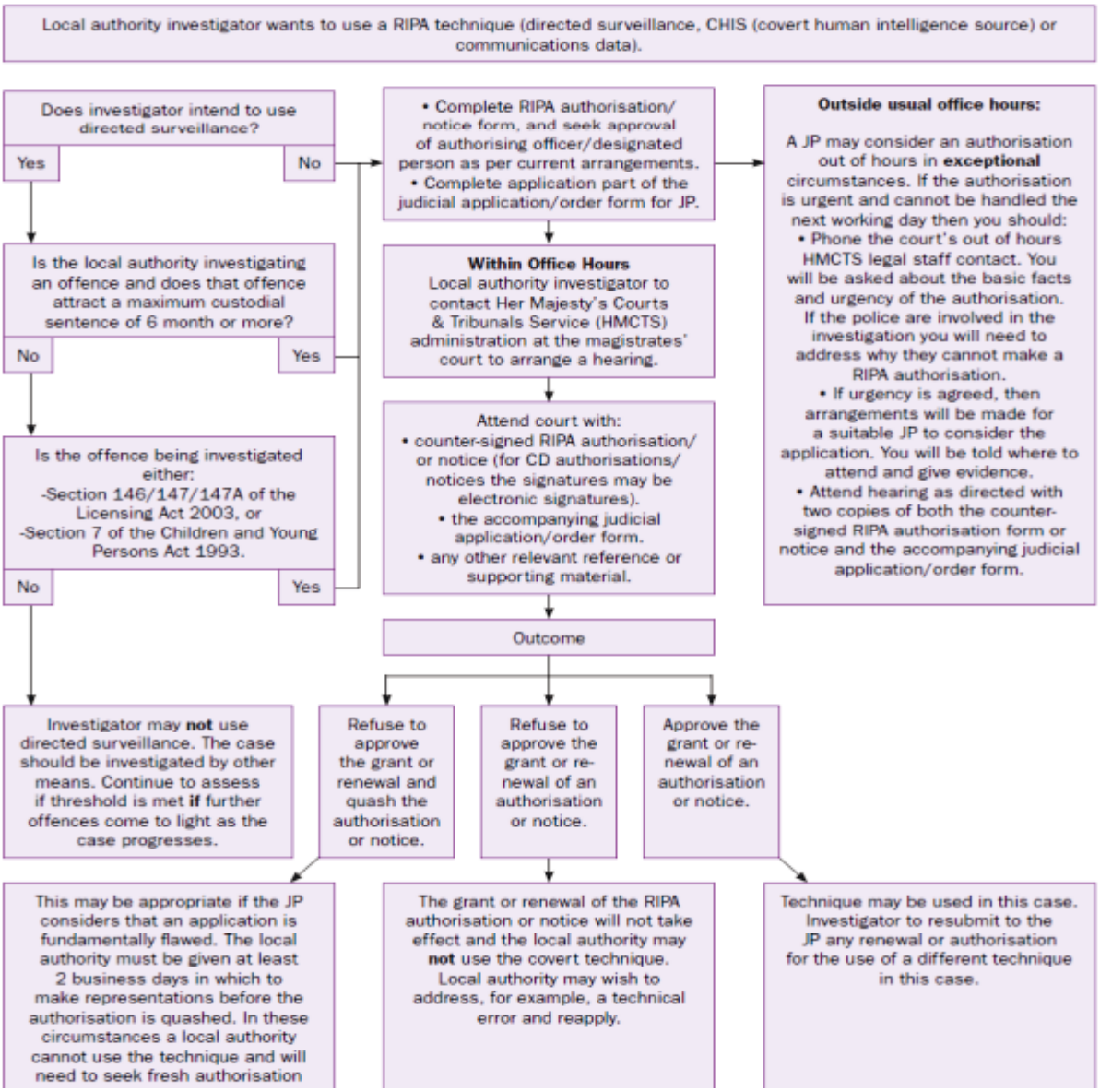
B. Only the Chief Executive is authorised to sign Forms relating to Juvenile Sources and Vulnerable Individuals (see Section G of this Document).

C. If a Director or Head of Service wishes to add, delete or substitute a post, s/he must refer such request to the Legal Services for consideration, as necessary.

D. If in doubt, ask Legal Services BEFORE any directed surveillance and/or CHIS is authorised, renewed, rejected or cancelled.

APPENDIX 2

LOCAL AUTHORITY PROCEDURE: APPLICATION TO A JUSTICE OF THE PEACE SEEKING AN ORDER TO APPROVE THE GRANT OF A RIPA AUTHORISATION OR NOTICE



APPENDIX 3

RIPA A FORMS: DIRECTED SURVEILLANCE

Form A1: Application for authorisation to carry out directed surveillance.

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

Form A2: Review of Form A1.

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

Form A3: Cancellation of Form A1.

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

Form A4: Application for Renewal of Form A1.

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

NB: If in doubt, ask Legal Services BEFORE any directed surveillance and/or CHIS is authorised, renewed, cancelled or rejected.

APPENDIX 4

RIPA B FORMS: COVERT HUMAN INTELLIGENCE SOURCE (CHIS)

MANAGEMENT OF CHIS

1. **A CHIS might be a member of the public or an employee of the authority operating undercover. A CHIS who is a member of the public, once authorised, will be managed by an appointed "handler" and an appointed "controller". Oversight and management arrangements for undercover operatives will differ, in order to reflect the specific role of such individuals as members of public authorities. The role of handler will be undertaken by a person referred to as a" cover officer" and the role of controller will be undertaken by a "covert operations manager".**

2. **The "handler" will have day to day responsibility for:**

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

3. **The handler of a CHIS will usually be of a rank or position below that of the Authorising Officer.**

4. **The "controller" will normally be responsible for the management and supervision of the "handler" and general oversight of the use of the CHIS**

Tasking

5. **Tasking is the assignment given to the source by the persons defined at sections 29(5)(a) and (b) of the 2000 Act, asking him to obtain information, to provide access to information or to otherwise act, incidentally, for the benefit of the relevant public authority. Authorisation for the use or conduct of a source is required prior to any tasking where such tasking requires the source to establish or maintain a personal or other relationship for a covert purpose.**

6. **The person referred to in section 29(5) (a) of the 2000 Act will have day to day responsibility for:**

   - **dealing with the source on behalf of the authority concerned;**
   - **directing the day to day activities of the source;**
   - **recording the information supplied by the source; and**
   - **monitoring the source's security and welfare;**

7. **The person referred to in section 29(5) (b) of the 2000 Act will be responsible for the general oversight of the use of the source.**

8. In some instances, the tasking given to a person will not require the source to establish a personal or other relationship for a covert purpose. For example a source may be tasked with finding out purely factual information about the layout of commercial premises. Alternatively, a Trading Standards Officer may be involved in the test purchase of items which have been labelled misleadingly or are unfit for consumption. In such cases, it is for the relevant public authority to determine where, and in what circumstances, such activity may require authorisation. Where a Trading Standards Officer is tasked their Line Manager will generally assume the role of the person referred to in 2 above and the Business and Public Protection Manager will assume the role in 3 above.

9. It is not the intention that authorisations be drawn so narrowly that a separate authorisation is required each time the source is tasked. Rather, an authorisation might cover, in broad terms, the nature of the source's task. If this changes, then a new authorisation may need to be sought.

10. It is difficult to predict exactly what might occur each time a meeting with a source takes place or the source meets the subject of an investigation. There may be occasions when unforeseen action or undertakings occur. When this happens, the occurrence must be recorded as soon as practicable after the event and, if the existing authorisation is insufficient it should either be updated and re-authorised (for minor amendments only) or it should be cancelled and a new authorisation should be obtained before any further such action is carried out.

11. Similarly where it is intended to task a source in a new way or significantly greater way than previously identified, the persons defined at section 29(5) (a) or (b) of the 2000 Act must refer the proposed tasking to the authorising officer, who should consider whether a separate authorisation is required. This should be done in advance of any tasking and the details of such referrals must be recorded.

Management responsibility

12. Public authorities should ensure that arrangements are in place for the proper oversight and management of sources, including appointing individual officers as defined in section 29(5) (a) and (b) of the 2000 Act for each source.

13. The person responsible for the day-to-day contact between the public authority and the source will usually be of a rank or position below that of the authorising officer.

14. In cases where the authorisation is for the use or conduct of a source whose activities benefit more than a single public authority, responsibilities for the management and oversight of that source may be taken up by one authority or can be split between the authorities.

Security and welfare

15. When deploying a CHIS the authority must take into account the safety and welfare of that CHIS when carrying out actions in relation to an authorisation or tasking, and the foreseeable consequences to others of that tasking. Before authorising the

use or conduct of a CHIS, the Authorising Officer should 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, after the cancellation of the authorisation, should also be considered at the outset. Also, 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.

16. **The CHIS handler is responsible for bringing to the attention of the CHIS 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.**

17. **Where deemed appropriate, concerns about such matters must be considered by the authorising officer, and a decision taken on whether or not to allow the authorisation to continue.**

Form B1: Application for authorisation of the Use or Conduct of a Covert Human Intelligence Source (CHIS).

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

Form B2: Cancellation of Form B.1

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

Form B3: Review of Form B1.

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

Form B4: Application for Renewal of Form B 1.

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

NB: If in doubt, ask Legal Services BEFORE any directed surveillance and/or CHIS is authorised, renewed, rejected or cancelled.

APPENDIX 5

APPLICATION FOR JUDICIAL APPROVAL FOR AUTHORISATION

Application for judicial approval for authorisation to obtain or disclose communications data, to use a covert human intelligence source or to conduct directed surveillance. Regulation of Investigatory Powers Act 2000 sections 23A, 23B, 32A, 32B.

Local authority:.....

Local authority department:.....

Offence under investigation:.....

Address of premises or identity of subject:.....

.....

.....

Covert technique requested: (tick one and specify details)

Communications Data ☐

Covert Human Intelligence Source ☐

Directed Surveillance ☐

Summary of details

.....

.....

.....

.....

.....

.....

Note: this application should be read in conjunction with the attached RIPA authorisation/RIPA application or notice.

Investigating Officer:.....

Authorising Officer/Designated Person:.....

Officer(s) appearing before JP:.....

Address of applicant department:.....

.....

Contact telephone number:.....

Contact email address (optional):.....

Local authority reference:.....

Number of pages:.....

Order made on an application for judicial approval for authorisation to obtain or disclose communications data, to use a covert human intelligence source or to conduct directed surveillance. Regulation of Investigatory Powers Act 2000 sections 23A, 23B, 32A, 32B.

Magistrates' court:.....

Having considered the application, I (tick one):

☐ **am satisfied that there are reasonable grounds for believing that the requirements of the Act were satisfied and remain satisfied, and that the relevant conditions are satisfied and I therefore approve the grant or renewal of the authorisation/notice.**

☐ **refuse to approve the grant or renewal of the authorisation/notice.**

☐ **refuse to approve the grant or renewal and quash the authorisation/notice.**

Notes

.....

.....

.....

.....

.....

Reasons

.....

.....

.....

.....

.....

.....

Signed:

Date:

Time:

Full name:

Address of magistrates' court: