Corporate Policy and Resources
Date: 27th July 2017

Subject: Review of The Regulation of Investigatory Powers (RIPA) Policy

Report by:	Chief Operating Officer
Contact Officer:	Alan Robinson Monitoring Officer T: 01427 676509
Purpose / Summary:	To Approve the revised Regulation of Investigatory Powers

RECOMMENDATIONS:

1)That members review and approve the attached Regulations of Investigatory Powers Act Policy

2)That members delegate authority to the Chief Operating Officer in consultation with the Chair of Policy and Resources to make housekeeping changes to this policy when necessary

IMPLICATIONS

Legal: Where it is necessary to carry out Covert Surveillance as part of an investigation it is a legal requirement to abide by the Regulations of Investigatory Powers Act.

Financial : FIN/56/18/TJB

None from this report

Staffing : All appropriate staff will require refresher training

Equality and Diversity including Human Rights : N/A

Risk Assessment :

The implementation of this policy is designed to mitigate the risk of Court actions being lost as a result of evidence being inadmissible.

Climate Related Risks and Opportunities : None

Title and Location of any Background Papers used in the preparation of this report:

Call in and Urgency:

Is the decision one which Rule 14 of the Scrutiny Procedure Rules apply?

Yes		**No**	✓

Key Decision:

Yes		**No**	✓

1 Context

1.1 The Regulations of Investigatory Powers Act (RIPA) is the law which governs the use of covert surveillance in carry out investigations. West Lindsey District Council is required to abide by the legislation and have a policy which is kept up to date

1.2 Any evidence gathered through Covert Surveillance without adhering to RIPA requirements would be inadmissible in court

1.3 This Policy once approved will give guidance to all appropriate officers on how to make use of the powers

1.4 West Lindsey may use these powers to investigate a varied range of offences however the powers are rarely used in practice as they are only used when no alternative to covert surveillance can be found

2 The Policy

2.1 The Policy is attached at appendix 1

2.2 This Policy is intended to set out how West Lindsey will abide by the RIPA provisions

2.3 It gives details of the roles of officers and their responsibilities in this area. All Covert Surveillance has to go through a stringent approval process which cumulates with apply to the Magistrates Court.

2.4 Records have to be managed and regularly reviewed.

3 Roles

3.1 There are 5 distinct roles which are dealt with in the Policy.

3.2 Applicants for authority to carry out covert surveillance are normally investigator

3.3 Authorising Officers are responsible for giving authority for the use of the Powers. It is proposed that there will be two nominated authorising officers. These will be the Director of Resources and Democratic and Corporate Governance Manager.

3.4 The RIPA monitoring officer will be the Council's Monitoring Officer

3.5 The Senior Responsible Officer will be the Chief Operating Officer

3.6 The role of gatekeeper is carried out Lincolnshire Legal Services

4 Conclusion

4.1 This policy is compliant with the requirements of RIPA and once approved this will be published on the Councils website.

4.2 General training for 18 officers was carried out on 10th July 2017

4.3 Training for the Monitoring Officer, Senior Responsible Officer and Authorising Officers is planned for 16th October 2017.

CORPORATE POLICY & PROCEDURES DOCUMENT

ON

THE REGULATION OF INVESTIGATORY POWERS ACT 2000 (RIPA)

UPDATED July 2017

CONTENTS PAGE Page No.

NB:
The Regulation of Investigatory Powers Act 2000 ('RIPA') refers to 'Designated Officers'. For ease of understanding and application within West Lindsey District Council, this Corporate Policy & Procedures Document refers to 'Authorised 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 Authorised Officers refer to 'Designated Officers' under RIPA.

A. Introduction and Key Messages

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

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 Shared Legal Services Office for advice and guidance. Appropriate training will be provided or organised by the Council to Authorised Officers and any other appropriate persons.

3. To ensure easy access, a copy of this Document will be placed on the website. The act itself and the Codes of Practice on Covert Surveillance and Covert Human Intelligence Sources will made available for officers on the Councils Intranet site and for members of the public on demand.

4. The Chief Operating Officer is the Senior Responsible Officer for RIPA and such will responsible for ensuring all officers work with the requirements of the law and fulfil their roles appropriately

5. The Council's Monitoring Officer will act as the RIPA Monitoring Officer. They will maintain and check the Central Register of all RIPA authorisations, reviews, renewals, cancellations and rejections. However, it is the responsibility of the relevant Authorising Officer to ensure that RIPA Monitoring Officer receive a copy of the relevant form within 1 week of the authorisation, review, renewal, cancellation or rejection.

6. RIPA and this Document are important for the effective and efficient operation of the Council's actions with regard to covert surveillance and Covert Human Intelligence Sources. This Document will, therefore, be kept under annual review by the RIPA Monitoring Officer. Additionally annual reports will be made by the RIPA Monitoring Officer to the relevant elected members of the Council to ensure that the policy is still fit for purpose and consistent with Council policies.

7. In terms of monitoring e-mails and internet usage, it is important to recognise the important interplay and overlaps with the 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.

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

B. West Lindsey District Council Policy Statement

1. The 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 RIPA Monitoring Officer, will keep this Document up to date and amend, delete, add or substitute relevant provisions, as necessary. The Chief Operating Officer will be the Senior Responsible Officer for this work.

C. RIPA Monitoring Officer Responsibilities

1. The Councils Monitoring Officer is the designated RIPA Monitoring Officer with overall authority for monitoring and keeping under review the Council's use of and compliance with the Regulation of Investigatory Powers Act 2000 and all amendments thereto and Codes of Practice issued under the said Act in consultation with the Chief Operating Officer

2. The RIPA Monitoring Officer also has responsibility for maintaining the Central Register for RIPA authorisations and oversight and quality control of the authorisation process, which will include the examination of authorisations to ensure they are compliant with current legislation and codes of practice and raising any issues as to the quality of authorisations with the authorising officers.

3. The RIPA Monitoring Officer will be responsible for the provision of training and maintenance of a Training Register for staff identified as requiring the same and for ensuring that all Directors and Authorised Officers are provided with updates on policy and guidance pertaining to RIPA.

4. The RIPA Monitoring Officer will have responsibility for raising awareness of RIPA within the Council and ensure that this policy is subject to annual review and that quarterly reports are made as to fitness for purpose to the relevant elected members.

5. The RIPA Monitoring Officer will be responsible for engaging with the Surveillance Commissioners and Inspectors when inspections are conducted and oversee the implementation of any post inspection action plans recommended or approved by them.

D. Authorised Officer and Director Responsibilities

1. This Corporate Policy and Procedures Document will become operative from 1st August 2017. It is important therefore, that relevant Directors, Strategic Leads, and Authorised 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 each Director/Strategic Lead to ensure their relevant members of staff who require training are identified and undertake suitable training as 'Applicants' through the RIPA Monitoring Officer and are kept up to date with policy and guidance information provided by the RIPA Monitoring Officer so as to avoid errors in the operation of the process and completion of the relevant forms.

3. Directors/Strategic Leads 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. Authorised 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 Authorised 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 Authorised Officer is in any doubt, s/he should obtain prior guidance on the same from his/her Chief Officer, the Council's Health & Safety Officer and/or the Legal Services Section.

5. Authorised Officers are encouraged, although not obliged, to use the services of Lincolnshire County Council Legal Shared Services who have agreed to act as 'gatekeeper' for applications to conduct surveillance activity. The gatekeeper role will involve LCC Trading Standards reviewing an application to conduct surveillance on behalf of an Authorised Officer of West Lindsey and providing advice and/or recommendations as appropriate on how the application may be enhanced **before** submission to the Magistrates Court to maximise the likelihood of it gaining approval. In certain circumstances, Lincolnshire County Council Trading Standards Department may recommend to the Authorised Officer that an application is not progressed and/or withdrawn. Authorised Officers must ensure that all documentation is sent using secure and confidential means as detailed in 6 below or via secure email to Mark.Keal@lincolnshire.gcsx.gov.uk .

6. Authorised 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.**

7. The Director of Resources will be the Authorising Officer for all RIPA applications. The deputy Authorising Officer will be the Council's Deputy Monitoring Officer

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 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 Council may interfere in the citizen's right mentioned above, if such interference is:-

   (a) **in accordance with the law;**

   (a) **necessary** (as defined in this Document); **and**

   (b) **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. 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 Council are covered by the Act for the time they are working for the 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 Authorised Officers. (Authorised 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 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 RIPA Monitoring Officer.

6. A flowchart of the procedures to be followed – for Directed Surveillance and the use of Covert Human Intelligence Sources (CHIS's)

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.

2. **RIPA does not**:

- make unlawful conduct which is otherwise lawful.

- prejudice or dis-apply any existing powers available to the Council to obtain information by any means not involving conduct that may be authorised under this Act. For example, it does not affect the 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 Authorised Officer or any Applicant is in any doubt, s/he should speak to a representative from the Shared Legal Services section **BEFORE** authorising, renewing, cancelling or rejecting any directed surveillance or use of a CHIS.

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 <u>overt</u> or <u>covert</u>.

2. ***Overt Surveillance***

Most of the surveillance carried out by the Council will be done overtly – there will be nothing secretive, clandestine or hidden about it. In many cases, Officers who are going about the usual business and just happen to observe something happening that represents a breach of legislation enforced by the Council, and/or will be going about Council business openly (e.g. carrying out a site visit pursuant to an existing power to inspect) or where the Council employs the use of CCTV cameras clearly apparent to the public for the surveillance of general behaviour and not targeted at a specific individual or group of individuals.

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 a licence is issued for the sale of alcohol 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 <u>unaware</u> of it taking place. (Section 26(9) (a) of RIPA).

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

6. ***Directed Surveillance***

Directed Surveillance is surveillance which:-

- is <u>covert;</u> and

- is not <u>intrusive surveillance</u> (see definition below – the Council must not carry out any <u>intrusive</u> 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 'Authorised Officers' for the purpose of RIPA can authorise 'Directed Surveillance' IF, AND ONLY IF, the RIPA authorisation procedures detailed in this Document 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**. **Council Officers must not carry out intrusive surveillance.**

12. **Proportionality**

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 should be chosen; and
- collateral intrusion involves invasion of third parties privacy and should, so far as is possible, be minimised.

Extra care should also be taken over any publication of the product of the surveillance.

13. **Further guidance** on surveillance can be found in the Home Office's statutory Code of Practice on Surveillance at www.homeoffice.gov.uk/crimpol/crimreduc/regulation/codesofpractice.html

Examples of different types of Surveillance

Type of Surveillance	**Examples**
Overt	• Police Officer or Community Officers 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 site visits where the officer is carrying out an open inspection of a site pursuant to a statutory power.
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 **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 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 Council is permitted to authorise the use of Juvenile Sources, as there are other onerous requirements for such matters.

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 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.

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. Recording sound (with a DAT recorder) on private premises could constitute intrusive surveillance, unless it is done overtly. For example, it will be possible to record if the noisemaker is warned that this will occur if the level of noise continues. Placing a stationary or mobile video camera outside a building to record anti social behaviour on residential estates will require prior authorisation.

12. **Further Information**

Further guidance on CHIS's can be found in the Home Office's statutory Code of Practice on the Use and Conduct of CHIS's at
www.homeoffice.gov.uk/crimpol/crimreduc/regulation/codesofpractice.html

I. 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.

Authorised Officers

2. Forms can only be signed by Authorised Officers, authorised to do so by the Council. Authorised posts are listed in **Appendix 1**. This Appendix will be kept up to date by the RIPA Monitoring Officer, and added to as needs require. If a Director wishes to add, delete or substitute a post, s/he must refer such request to the RIPA Monitoring Officer for consideration, as necessary. The RIPA Monitoring Officer 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!**

Training Records

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

Application Forms

6. Only the approved RIPA forms set out in this Document must be used. Any other forms used will be rejected by the Authorised Officer and/or Legal Services.

Grounds for Authorisation

7. Directed Surveillance **(A Forms),** the Conduct and Use of a CHIS **(B Forms**), can only be authorised by the 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

8. Before an Authorised Officer signs a Form, **s/he must**:-

   (a) Be mindful of this Corporate Policy & Procedures Document, the Training provided by and any other guidance issued, from time to time, by RIPA Monitoring Officer 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 other appropriate means of gathering the information. **The least intrusive method will be considered proportionate by the courts.**

(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) /Year/Number of Application

(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 Monitoring 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.

(h) The authorised officer is encouraged to seek advice from Lincolnshire County Council Trading Standards on the quality of the application before them, prior to submission to the Magistrates Court, using the procedure outlined at number 5 on page 6 of this procedure.

Additional Safeguards when Authorising a CHIS

9. When authorising the conduct or use of a CHIS, the Authorised Officer **must also:-**

(a) be satisfied that the **conduct** and/or **use** of the CHIS is proportionate 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

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

Urgent Authorisations

10. Urgent authorisations should not ordinarily be necessary. In exceptional circumstances, however, urgent authorisations may be given orally if the time that would elapse before a written authorisation can be granted would be likely to endanger life or jeopardise the investigation or operation for which the authorisation was being given.

11. It will not be urgent where the need for authorisation has been neglected or is of the Officer's own making.

12. Urgent authorisations last for no more than 72 hours. They must be recorded in writing on the standard form as soon as practicable and the extra boxes on the form completed to explain why the authorisation was urgent.

Duration

13. The Form **must be reviewed in the time stated and cancelled** once it is no longer needed. The 'authorisation' to carry out/conduct the surveillance lasts for a maximum of 3 months (from authorisation) for Directed Surveillance, and 12 months (from authorisation) for a CHIS. However, whether the surveillance is carried out/conducted or not, in the relevant period, does not mean the 'authorisation' is 'spent'. In other words, **the Forms do not expire!** The forms have to be reviewed and/or cancelled (once they are no longer required)!

14. Urgent oral authorisation, if not already ratified in a written authorisation, will cease to have effect after 72 hours, beginning with the time when the authorisation was granted.

15. Authorisations can be renewed in writing when the maximum period has expired. The Authorising Officer must consider the matter afresh, including taking into account the benefits of the surveillance to date, and any collateral intrusion that has occurred.

16. The renewal will begin on the day when the authorisation would have expired. In exceptional circumstances, renewals may be granted orally in urgent cases and last for a period of seventy-two hours and must be recorded in writing on the standard forms as soon as practicable explaining why the renewal was urgent.

J. Working With/Through Other Agencies

1. When some other agency has been instructed on behalf of the Council to undertake any action under RIPA, this Document and the correct forms 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. When some other agency (e.g. Police, Customs & Excise, and Inland Revenue etc):-

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

   (b) 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 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 Council's co-operation in the agent's RIPA operation. In such cases, however, the Council's own RIPA forms should not be used as the 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 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. Copies of letters should be sent as soon as possible to the RIPA Monitoring Officer for retention.

4. Where it is foreseen that other agencies will be involved in carrying out any surveillance, these agencies should be detailed in the application.

If in doubt, please consult with Legal Services at the earliest opportunity.

K. Record Management

1. **The 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 the RIPA Monitoring Officer.**

2. ***Records maintained in the Department***

The following documents must be retained by the relevant Authorising 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 Authorised 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 Authorised Officer;
- the Unique Reference Number for the authorisation (URN).

3. Each form will have a URN. The departmental representative will issue the relevant URN to Applicants. The cross-referencing of each URN takes place within the forms for audit purposes.

Central Register maintained by the RIPA Monitoring Officer

4. Authorised Officers must forward details of each form to the RIPA Monitoring Officer for the Central Register, within 1 week of the authorisation, review, renewal, cancellation or rejection. The RIPA Monitoring Officer will monitor the same and give appropriate guidance, from time to time, or amend this Document, as necessary.

5. The Council will retain 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 Council's policies and procedures, and individual authorisations.

6. The following information will be retained for a period of three years and up-dated each time an authorisation is granted, renewed or cancelled and should be available for inspection on the request of a Commissioner or Inspector of the Surveillance Commissioners Office: This should be a separate record for the authorisation of Directed Surveillance and CHIS and should contain the following information in relation to both forms of application:

- 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;
- Whether the urgency provision was used and if so why;
- 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 **directed surveillance authorisations** the following documentation should be centrally retrievable for a period of three years:

- Copies of all applications, authorisations and any supplementary documentation and notifications of approval given by the authorising officer;
- 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 **CHIS authorisations** the following documentation should be centrally retrievable for a period of three years:

- A copy of authorisations, notifications of approval and renewals together with any supporting documentation;
- The reasons why the person renewing an authorisation considered it necessary to do so;
- Any authorisation which was granted or renewed orally (in an urgent case) and the reason why the case was considered urgent;
- 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.

L. Concluding Remarks

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. Authorised 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 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 Procedures.

For further advice and assistance on RIPA, please contact the Legal Service's Office.

M. Complaints

1. Complaints relating to covert surveillance must be investigated in accordance with the Council's complaints policy.

2. The Authorising Officer of the 'covert surveillance subject of complaint' will not carry out the investigation of that complaint.

RIP 1

PART II OF THE REGULATION OF INVESTIGATORY POWERS ACT (RIPA) 2000

APPLICATION FOR AUTHORISATION TO CARRY OUT DIRECTED SURVEILLANCE

Public Authority (Including full address)	

Name of applicant		**Unit/Branch/Division**	
Full Address			
Contact Details			
Investigation/ Operation Name		**Operation Reference Number** (File number**)**	
Investigating Officer (if a person other than the applicant)			

Details of application:

1. Give rank or position of authorising officer in accordance with the Regulation of Investigatory Powers (Directed Surveillance and Covert Human Intelligence Sources) Order 2003; No. 3171[1]

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

[1] For local authorities: The exact position of the authorising officer should be given. For example Head of Trading Standards.

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

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

Name

Address:

DOB:

Other information as appropriate:

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

6. Identify on which grounds the directed surveillance is <u>necessary</u> under Section 28 (3) of RIPA. Delete those that are inapplicable. Ensure that you know which of these grounds you are entitled to rely on (SI 2003 No. 3171)

- In the interests of national security;

- *for the purpose of preventing or detecting crime or preventing disorder (*the only ground for WLDC);

- In the interests of the economic well-being of the United Kingdom

- in the interest of public safety

- for the purpose of protecting public health;

- for the purpose of assessing or collecting any tax, duty, levy or other imposition, contribution or charge payable to a government department.

7. Explain <u>why</u> this directed surveillance is necessary on the grounds you have identified (Code paragraph 2.4)

8. Supply details of any potential collateral intrusion and why the intrusion is unavoidable (Bear in mind Code paragraphs 2.6 to 2.10) **Describe precautions you will take to minimise collateral intrusions**

9. Explain <u>why</u> this directed surveillance is proportionate to what it seeks to achieve. How intrusive might it be on the subject of surveillance or on others? And why is this intrusion outweighed by the need for surveillance in operational terms or can the evidence be obtained by any other means? (Code paragraph 2.5)

10. Confidential Information (Code paragraphs 3.1 to 3.12) **Indicate the likelihood of Acquiring any Confidential Information:**

11. Applicants details			
Name:		**Telephone number:**	
Grade/Rank:		**Date:**	
Signature:			

12. Authorising Officer's Statement (Spell out the "5 Ws" – Who; What; Where; When; Why and HOW – in this and the following box.)
I hereby authorise directed surveillance defined as follows: (Why is the surveillance necessary, whom is the surveillance directed against, Where, When will it take place, What surveillance activity/equipment is sanctioned, How is it to be achieved?)

13. Explain <u>Why</u> you believe the directed surveillance is necessary (Code paragraph 2.4) Explain <u>Why</u> you believe the directed surveillance to be proportionate to what is sought to be achieved by carrying out (Code paragraph 2.5)

14. (Confidential Information Authorisation) Supply detail demonstrating compliance with Code paragraphs 3.1 to 3.12			
Date of first review			
Programme for subsequent reviews of this authorisation (Code paragraph 4.22). Only complete this box if review dates after first review are known. If not or inappropriate to set additional review dates then leave blank			
Name:		**Grade/Rank:**	
Signature:		**Date and Time:**	
Expiry date and time (e.g. authorisation granted on 1 April 2005 – expires 30 June			

15. Urgent authorisation (Code paragraphs 4.17 and 4.18): Authorising Officer: explain why you considered the case so urgent that an oral instead of a written authorisation was given.			
16. If you are only entitled to act in urgent cases: explain why it was not reasonably practicable for the application to be considered by a fully qualified authorising officer			
Name:		**Grade/Rank:**	
Signature:		**Date/Time:**	
Urgent Authorisation Expiry Date:		**Expiry Time**	
Remember the 72 hour rule for urgent authorities (Check Code of Practice)	e.g. authorisation granted at 5pm on June 1st expires 4.59 pm on 4th June		

APPENDIX 2

RIP 2

PART II OF THE REGULATION OF INVESTIGATORY POWERS ACT (RIPA) 2000

Public Authority (including full address)	

Name of applicant		**Unit/Branch/Division**	
Full address			
Contact details			
Investigation/ Operation name		**Operation reference number** (file number)	
Renewal number			

Details of renewal:

1. Renewal numbers and dates of any previous renewals	
Renewal number	**Date**

2. Detail any significant changes to information as listed in the original application as it applies at the time of the renewal

3. Detail the reasons why it is necessary to continue with the directed surveillance

4. Detail why the directed surveillance is still proportionate to what it seeks to achieve

5. Indicate the content and value to the investigation or operation of the product so far obtained by the directed surveillance

6. Give details of the results of the regular reviews of the investigation or operation

7. Applicant's details			
Name:		**Telephone number:**	
Grade/Rank:		**Date:**	
Signature:			

8. Authorising Officer's comments <u>This box must be completed</u>

9. Authorising Officer's statement			
I, (insert name) hereby authorise the renewal of the directed surveillance operation as detailed above. The renewal of this authorisation will last for 3 months unless renewed in writing. This authorisation will be reviewed frequently to assess the need for the authorisation to continue.			
Name:		**Grade/Rank:**	
Signature:		**Date:**	
Renewal from - time:		**Date:**	

Date of First review	
Date of subsequent reviews of this authorisation	

RIP 3

PART II OF THE REGULATION OF INVESTIGATORY POWERS ACT 2000

CANCELLATION OF A DIRECTED SURVEILLANCE AUTHORISATION

Public Authority (Including full address)	West Lindsey District Council, Guildhall, Marshalls Yard Gainsborough, DN21 2NA

Name of Applicant		**Unit/Branch/Division**	Revenues (Fraud).
Full Address			
Contact Details			
Investigation/ Operation Name		**Operation Reference Number** (File number)	

Details of cancellation:

1. Explain the reason(s) for the cancellation of the authorisation

2. Explain the value of surveillance in the operation

3. Authorising Officer's Statement.			
I (insert name)hereby authorise the cancellation of the directed surveillance investigation/operation as detailed above			
Name:		**Grade/Rank:**	
Signature:		**Date:**	

4. Time and Date of when the authorising officer instructed the surveillance to cease			
Date:		**Time:**	

5. Authorisation Cancelled	**Date:**	**Time:**

APPENDIX 4

PART II REGULATION OF INVESTIGATORY POWERS ACT 2000

REVIEW OF A DIRECTED SURVEILLANCE AUTHORISATION

Public Authority (including full address)	

Name of Applicant		**Unit/Branch/Division**	Revenues (Fraud).
Full Address			
Contact Details			
Investigation/ Operation Name		**Operation Reference Number** (File number)	
Date of authorisation or last renewal		**Expiry Date of authorisation or last renewal**	

1. Review number and dates of any previous reviews	
Review Number	**Date**

2. Summary of the investigation/operation to date, including what private information has been obtained and the value of the information so far obtained

3. Detail the reason why it is necessary to continue with the directed surveillance

4. Explain how the proposed activity is still proportionate to what it seeks to achieve

5. Detail any incidents of collateral intrusion and the likelihood of any further incidents of collateral intrusions occurring

6. Give details of any confidential information acquired or accessed and the likelihood of acquiring confidential information

7. Applicant's details			
Name:		**Telephone number:**	
Grade/Rank:		**Date:**	
Signature:			

8. Review Officer's Comments, including whether or not the directed surveillance should continue.

9. Authorising Officer's statement			
I (insert name) hereby agree that the directed surveillance investigation/operation as detailed above [*should/should not] continue [until its next *review/renewal] [it should be cancelled immediately] ***Delete as appropriate.**			
Name:		**Grade/Rank:**	
Signature:		**Date and Time:**	

10. Date of next review	

The layout and guidance of this RIP form is subject to change. Any changes to procedures or guidance will be notified in writing.

APPENDIX 5

CHANGE OF CIRCUMSTANCES FORM RIP5

PART II REGULATION OF INVESTIGATORY POWERS ACT 2000
DIRECTED SURVEILLANCE

Operation Name	
Operation Reference Number	

Date change occurred/notified	

1. Particulars of subject(s) who have been added to the scope of the RIP application	
Name: ID Details Address: NINO D.O.B	Name: ID Details Address: NINO D.O.B

2. Particulars of subject(s) who have been removed from the scope of the RIP application	
Name: ID Details Address: NINO D.O.B	Name: ID Details Address: NINO D.O.B

3. Particulars of subject(s) whose identity has been established	
Subject ref: Name: Address: NINO D.O.B	Subject ref: Name: Address: NINO D.O.B

4. Particulars of other changes

5. What impact has change of circumstances had on the scope of the RIP authorisation

6. If surveillance is to continue, provide an update of operational objectives and plan of action. If not, RIP 3 must be completed to accompany Change of Circumstances form

7. Applicant details			
Name:		**Telephone number:**	
Grade/Rank:		**Date:**	
Signature:			

8. Countersigning Officer's comments (where applicable)			
Name:		**Grade/Rank:**	
Signature:		**Date:**	

9. Authorising Officer's comments

10. Authorising Officer's statement			
I hereby *authorise/refuse the continuation of the directed surveillance operation as detailed above. (*delete where authorisation is refused)			
Name:		**Grade/Rank:**	
Signature:		**Date (and Time)**	

11. Urgent authorisation: Details of why change of circumstances request is urgent			
Name:		**Grade/Rank:**	
Signature:		**Date/Time:**	

12. Authorising Officer's comments (This must include why the authorising officer or person entitled to act in their absence considered the case urgent)			
Name:		**Grade/Rank:**	
Signature:		**Date:**	