APPENDIX A

served by One Team

East Lindsey District Council and Boston Borough Council Policy and procedures on the Regulation of Investigatory Powers Act 2000 (RIPA)

Version 5 – July 2021

Table of Contents:

1. Introduction

This Policy sets out the Councils position in relation to the Regulation of Investigatory Powers Act 2000 (RIPA), which established a statutory framework for the regulation of covert surveillance by, amongst others, local authorities. The Act is designed as a mechanism to provide the correct balance between an individual's right to privacy and proper use of data and surveillance, having due regard to human rights as defined in the Human Rights Act 1998.

The procedures and guidance set out in this policy are based on the provisions of RIPA; Home Office Codes of Practice and guidance issued by the Investigatory Powers Commissioner's Office. Links to Guidance can be found at the end of this Policy.

Officers of the Councils should be aware of the scope and extent of activities covered by RIPA.

As a company separate from the Councils (albeit one that is wholly owned by the Councils) employees or Agents of Public Sector Partnership Services Ltd (PSPS) cannot authorise covert surveillance but can seek such authorisation from either Council in adherence to this Policy.

What RIPA does:

- Require prior authorisation and judicial approval of directed covert surveillance and use of covert human intelligence source (CHIS)
- Prohibit the Councils from carrying out intrusive Surveillance
- Require appropriate consideration and safeguards

What RIPA does not;

- Prejudice existing powers available to the Councils that do not involve RIPA conduct e.g. to obtain information from the DVLA or HMLR
- Authorise the use of Directed Surveillance unless the Crime threshold is met.

2. Policy Statement

The Councils are committed to building a fair and safe community for all by ensuring the effectiveness of laws designed to protect individuals, businesses, the environment and public resources.

The Councils recognise that the vast majority of individuals comply with the law. For those that choose not to the Councils have a responsibility to ensure firm but fair enforcement action is taken which may include authorised covert surveillance in order to gather evidence of illegal activity.

Where any such surveillance is contemplated by officers it must be authorised under the Act to ensure it is lawful and does not infringe a person's human rights.

The Councils will not use covert surveillance unless it is absolutely **necessary** to

achieve the desired aims and only so long as it is **proportionate** to do so and is done in a proportionate manner and with adequate regard to the rights and freedoms of those who are not a target of the covert surveillance.

The Councils **will** when using covert surveillance:

- have due regard to the following legislation:
    - Human Rights Act 1998
    - Regulation of Investigatory Powers Act 2000
    - Protection of Freedoms Act 2012
    - Data Protection Act 2018
    - UK General Data Protection Regulation
- actively monitor its use
- have due regard to the Home Office Codes of Practice
- ensure authorisations are granted by the appropriately trained and designated officers
- ensure staff and (contractors) are properly trained
- properly investigate any complaints about its use

The Councils will **not**:

- normally use Covert Human Intelligences Sources (CHIS). Any need to employ a CHIS must be authorised by the Chief Executive
- carry out intrusive surveillance within the meaning of RIPA
- use covert surveillance (regulated by RIPA) unless judicial approval has been obtained

2.1 Purpose

This Policy sets out the practice to be followed before any covert surveillance is undertaken when carrying out investigations and it will assist officers in understanding:

- when surveillance is regulated by RIPA
- when authorisation criteria are met
- RIPA procedures
- implications of the Codes of Practice
- non-RIPA surveillance
- how to complete forms

2.2 Procedure

All covert surveillance shall be set out in accordance with the procedures in this Policy.

<u>The following documents must be maintained:</u>

- Copies of applications and authorisations and any supporting documents and the approval of the Authorising Officer (AO)
- Copy of any authorisation made by the judiciary
- A record of the period of surveillance
- The frequency of reviews by the AO and a record of that review
- A copy of any renewal of any authorisation (by AO or Judiciary)
- Date, time and details of any instructions given by the AO

Approved Forms:

Once the type of surveillance has been decided then the appropriate form can be completed and sent to the Authorising Officer for approval. Forms can be downloaded here along with appropriate guidance for each application:

https://www.gov.uk/government/collections/ripa-forms--2

Central Register:

A central register must be kept by the RIPA coordinator detailing:

- Date and type of any authorisation
- Date any order made by a Justice of the Peace
- Name and grade of AO
- Unique ref number of the investigation
- Brief description and names of subjects of investigation
- Whether any urgency provisions were used and why
- Exactly what is authorised
- Details of any renewal
- Whether confidential information is likely to be obtained
- Confidential information (if any)
- Date of cancellation
- Self-authorisation
- Reviews
- Original copies of any documents

Records Retention:

All documents should be marked as confidential and the RIPA coordinator is responsible for their retention, security and destruction. In accordance with the Council's data Protection Policies and the RIPA Codes of Practice. The retention period is five years from the ending of the period authorised.

2.4 Training and review

All Council officers undertaking covert surveillance shall be appropriately trained to ensure they understand their legal obligations. Authorising Officers shall attend appropriate training for that role at least every three years

This Policy will be reviewed every three years by the Senior Responsible Officer (SRO) who will make an annual report to the Audit and Governance Committee at

each Council, on any amendments to the Policy and any surveillance carried out within the previous year.

3.0 Activity Requiring Authorisation

3.1 The following types of activity will require authorization:

- Directed Surveillance
- The conduct and use of a CHIS *(not usually used by Councils)*

3.2 Directed surveillance is any activity undertaken covertly for the purpose of a specified investigation, in such a way that it is likely to obtain information about a person's private life

3.3 A covert human intelligence source (CHIS) is an inside informant or undercover officer (including someone who develops or maintains a relationship with the target) having a covert purpose of obtaining or accessing information for the investigator.

4.0 Applying for Authorisations

4.1 Only Authorising Officers (AO's) can enable an application under the Act. These persons are listed in appendix 3.

4.2 AO's may authorise for any service within the Councils and PSPS Limited (the Councils data processor)

4.3 To apply the investigator should select and complete the appropriate application form from the link above and send securely to the AO. Guidance and documents can be found by following the link.

4.4 All information should be marked as Confidential when sent to the AO.

4.5 The investigator should include all steps taken so far in the investigation and any steps to be taken if the authorisation is made so that it is clear what the authorisation is for.

5.0 Granting of Authorisations by AO

5.1 Section 28 of RIPA states: *a person shall not grant an authorization for directed surveillance unless he believes that authorisation is:*

> *(a) necessary for the purpose of preventing or detecting crime, or of preventing disorder involving a crime; and*
>
> *the authorised surveillance is proportionate to what is sought to be achieved by it.*

There is a **crime** threshold to be reached, i.e. the criminal offence:

- is or would be punishable (whether on summary conviction or on indictment) by a maximum term of at least 6 months of imprisonment, or
- it arises from the underage sale of alcohol, tobacco, or nicotine inhaling products.

5.2 The Authorising Officer, in determining whether the surveillance is proportionate, will give particular consideration to any collateral intrusion on, or interference with, the privacy of persons other than the subject(s) of the surveillance.

Such consideration of proportionality must involve:

- **balancing** the size and scope of the proposed activity against the gravity and extent of the perceived crime or harm;
- **explaining** how and why the methods to be adopted will cause the least possible intrusion on the subject and others;
- **considering** whether the activity is an appropriate use of the legislation and a reasonable way, having considered all reasonable alternatives, of obtaining the information sought;
- **evidencing**, as far as reasonably practicable, what other methods had been considered and why they were not implemented, or have been implemented unsuccessfully.

The Home Office Code of Practice on Covert Surveillance and Property Interference should be considered on the issue of proportionality (paragraphs 4.5 and 4.6):

https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/742041/201800802_CSPI_code.pdf

5.3 Authorisations must be given in writing.

It is possible that Authorising Officers may face cross-examination in court about the authorisation some time after it is granted, and memories fade. It is therefore important that a full written record of what they are being asked to authorise, appears on the application form. If in doubt, Authorising Officers should ask for more detail.

5.4 Authorising Officers should not be responsible for authorising their own activities or that of their own service areas.

5.5 All RIPA authorisations must be approved by a Magistrate before an authorisation becomes effective and directed surveillance is undertaken, or a CHIS deployed.

5.6 Duration of Authorisations and Reviews

An authorisation in writing ceases to have effect at the end of a period of 3 months beginning with the day on which it took effect, e.g. an authorisation starting 1st January would come to an end on 31st March.

Regular reviews of authorisations should be undertaken. The results of the review should be recorded on the appropriate form and a copy filed on the central record of authorisations and any paper copies are to be held in the CCTV Control Room at Boston Borough Council. If the surveillance provides access to confidential information or involves collateral intrusion, more frequent reviews will be required. The authorising officer should determine at the time of giving the initial authorisation, how often a review should take place (and this may also be subsequently reviewed).

5.7 Renewals

5.7.1 While an authorisation is still in force, the Authorising Officer can renew it if he considers this necessary for the purpose for which the authorisation was originally given. The authorisation will be renewed in writing for a further period, beginning with the day when the authorisation would have expired, but for the renewal, and can be for a period up to 3 months.

5.7.2 Applications requesting renewal of an authorisation are to be made on the appropriate form as set out at the appropriate form and submitted to the Authorising Officer.

The renewal must be granted before the original authorisation ceases to have effect.

5.7.3 Applications for renewal will record whether it is the first renewal; and if not, every occasion on which the authorisation has previously been renewed. Applications must also detail:

- the significant changes to the information in the initial authorisation
- the reasons why it is necessary to continue with the surveillance
- the content and value to the investigation or operation, of the information so far obtained by the surveillance
- The results of regular reviews of the investigation or operation.

5.7.4 When a directed surveillance authorisation requires renewal, the renewal must be approved by a magistrates' court in the same manner as an initial authorisation.

5.8 **Cancellations**

The person who granted or last renewed the authorisation (or other person with Authority under this policy) **MUST** cancel it if he is satisfied that the directed surveillance no longer meets the criteria for authorisation.

Requests for cancellation will be made on the appropriate form and submitted to the Authorising Officer for authorisation of the cancellation. All directed surveillance cancellations must include directions for the management and storage of any surveillance product.

6 Management Responsibility

The day to day contact between the Council and the source is to be conducted by the handler, who will usually be an officer below the rank of the Authorising Officer.

No vulnerable person or young person under the age of 18 should be used as a source.

Security and Welfare

Account must be taken of the security and welfare of the source. The Authorising Officer, prior to granting authorisation, should ensure that an assessment is carried out to determine the risk to the source of any task and the likely consequences should the target know the role of the CHIS.

Confidential Material

Where the likely consequence of the directed surveillance or conduct of a source would be for any person to acquire knowledge of confidential material, the deployment of a source should be subject to special authorisation. In these cases, the proposed course of conduct must be referred to the Head of Paid Service or (in his absence) a Director for a decision as to whether authorisation may be granted.

Monitoring of personal information online

The study of an individual's on-line presence may engage privacy considerations requiring RIPA authorisation. The attached Annex 2 gives guidance on the monitoring of information online, such as social media.

7. MAINTENANCE OF RECORDS

7.1 Each Service shall keep in a dedicated place

(a) a record of all authorisations sought
(b) a record of authorisations granted and refused

(c) applications for the granting, renewal and cancellation of authorisations

7.2 The records will be confidential and will be retained for a period of 3 years from the ending of the authorisation.

7.3 Each Authorising Officer shall send original copies of all applications/authorisations, reviews, renewals and cancellations to the RIPA Co-coordinating Officer, who will maintain a central record of all authorisations. The report will include details of the level of compliance with the requirements for authorisation.

7.4 Authorising Officers will ensure compliance with the appropriate data protection requirements and any relevant codes of practice produced by individual authorities in the handling and storage of material.

7.5 Where material is obtained by surveillance which is:

(a) wholly unrelated to a criminal or other investigation, or
(b) to the person subject of the surveillance, and
(c) there is no reason to believe it will be relevant to future civil or criminal proceedings it should be destroyed immediately. The decision to retain or destroy material will be taken by the relevant Authorising Officer.

8.0 Training and awareness of the contents of the Act

It shall be the responsibility of each Service Manager, or an Authorised Officer for that service, to ensure that all staff involved or likely to be involved in investigations, are adequately trained so as to be aware of the requirements and implications of the Act.

It shall be the responsibility of the Senior Responsible Officer with the assistance of the RIPA Co-coordinating Officer to ensure that all relevant officers have received appropriate training and are aware of the requirements and implications of the Act.

9. Non-RIPA Surveillance

From time to time a local authority may wish to undertake covert surveillance,which is not regulated by RIPA. This is fine as RIPA is permissive legislation.

Where the matter being investigated falls outside of RIPA the procedure in this part of the Policy can be followed. It is important to remember that the Council's actions could be challenged both by claiming that the evidence obtained through non-RIPA surveillance is inadmissible or that the Council has infringed a person's civil liberties. This could lead to action being taken against the Council in the civil courts. A person might also complain to the Local Government and Social Care Ombudsman about the Council's actions. It is therefore very important that non-RIPA surveillance is only considered in appropriate cases and the appropriate non–RIPA authorisation is sought.

Authorisation under RIPA affords a public authority a defence under Section 27 i.e. the activity is lawful for all purposes. However, failure to obtain an authorisation does not make covert surveillance unlawful. S.80 states:

> *"Nothing in any of the provisions of this Act by virtue of which conduct of any description is or may be authorised by any warrant, authorisation or notice, or by virtue of which information may be obtained in any manner, shall be construed –*
>
> *(a) as making it unlawful to engage in any conduct of that description which is not otherwise unlawful under this Act and would not be unlawful apart from this Act;*
> *(b) as otherwise requiring—*
> - *the issue, grant or giving of such a warrant, authorisation or notice, or*
> - *the taking of any step for or towards obtaining the authority of such a warrant, authorisation or notice, before any such conduct of that description is engaged in; or*
>
> *(c) as prejudicing any power to obtain information by any means not involving conduct that may be authorised under this Act."*

This point was explained more fully by the Investigatory Powers Tribunal in the case of C v The Police (Case No: IPT/03/32/H 14th November 2006):

> *"Although RIPA provides a framework for obtaining internal authorisations of directed surveillance (and other forms of surveillance), there is no general prohibition in RIPA against conducting directed surveillance without RIPA authorisation. RIPA does not require prior authorisation to be obtained by a public authority in order to carry out surveillance. Lack of authorisation under RIPA does not necessarily mean that the carrying out of directed surveillance is unlawful."*

A local authority may wish to conduct "Non-RIPA Surveillance" for one of two reasons:

- Crimes Not Carrying Six Months Imprisonment and Employee Surveillance

Since 1st November 2012, local authority Authorising Officers may not authorise Directed Surveillance unless it is for the purpose of preventing or detecting a criminal offence and it meets the condition set out in New Article 7A(3)(a) or (b) of the 2010 Order. Those conditions are that the criminal offence which is sought to be prevented or detected is punishable, whether on summary conviction or on indictment, by a maximum term of at least 6 months of imprisonment, or would constitute an offence under sections 146, 147 or 147A of the Licensing Act 2003 or section 7 of the Children and Young Persons Act 1933 (offences involving sale of tobacco and alcohol to underage children).

Covert surveillance that does not meet the six month Crime test.

This point is made by the ChiefSurveillance Commissioner in his annual report

(2010/2011):

> *"The higher threshold in the proposed legislation will reduce the number of cases in which local authorities have the protection of RIPA when conducting covert surveillance; it will not prevent the use of those tactics in cases where the threshold is not reached but where it may be necessary and proportionate to obtain evidence covertly and there will be no RIPA audit trail. Part I of RIPA makes unauthorised interception unlawful. In contrast, Part II makes authorised surveillance lawful but does not make unauthorised surveillance unlawful."*

Employee Surveillance

Most employee surveillance will not be authorisable under RIPA, if a previous decision by the Investigatory Powers Tribunal is to be followed.

In C v The Police and the Secretary of State for the Home Department (14th November 2006, No: IPT/03/32/H), C, a former police sergeant, retired in 2001 having made a claim for a back injury he sustained after tripping on a carpet in a police station. He was awarded damages and an enhanced pension due to the injuries.

In 2002, the police instructed a firm of private detectives to observe C to see if he was doing anything that was inconsistent with his claimed injuries. Video footage showed him mowing the lawn. C sued the police claiming they had carried out directed surveillance without an authorisation. The Tribunal first had to decide if it had jurisdiction to hear the claim. The case turned on the interpretation of the first limb of the definition of directed surveillance i.e. was the surveillance "for the purposes of a specific investigation or a specific operation?"

The Tribunal ruled that this was not the type of surveillance that RIPA was meant to regulate. It made the distinction between the ordinary functions and the core functions of a public authority:

> *"The specific core functions and the regulatory powers which go with them are identifiable as distinct from the ordinary functions of public authorities shared by all authorities, such as the employment of staff and the making of contracts. There is no real reason why the performance of the ordinary functions of a public authority should fall within the RIPA regime, which is concerned with the regulation of certain investigatory powers, not with the regulation of employees or of suppliers and service providers."*

The Tribunal also stated that it would not be right to apply RIPA to such surveillance for a number of reasons:

i. RIPA does not cover all public authorities, and there was no sense in police employee surveillance being conducted on a different legal footing than, for example, the Treasury, which does not have the same surveillance rights under RIPA.

ii. The Tribunal has very restrictive rules about evidence, openness and rights of appeal. The effect of these would lead to unfairness for employees of RIPA authorities when challenging their employers' surveillance as compared to those who were employed by non RIPA authorities.

This case suggests that, even where employee surveillance is being carried out on one of the grounds in section 28(3), the question has to be; is it for a core function linked to one of the authority's regulatory functions? In the local authority context this would include, amongst others, trading standards, environmental health and licensing. If it is not being done for one of these purposes it will not be directed surveillance.

Human Rights Compliance

Covert surveillance done without a RIPA authorisation will not have the protection of RIPA (i.e. the defence in section 27). However it will still be able to be undertaken as long as it is done in accordance with the European Convention on Human Rights (ECHR) which is directly enforceable against public authorities pursuant to the Human Rights Act 2018. Article 8 of the ECHR states:

> *"Everyone has the right to respect for his private and family life his home and his correspondence.*
>
> *There shall be no interference by a public authority with the exercise of this right except such as in accordance with the law and is necessary in a democratic society in the interests of public safety, for the protection of public order, health or morals, or for the rights and freedoms of others."*

To satisfy Article 8, the covert surveillance must be both necessary and proportionate. In deciding whether it is, the same factors need to be considered as when authorising surveillance regulated by RIPA.

Non-RIPA Data Protection Compliance

When carrying out covert surveillance of employees not regulated by RIPA, the Data Protection Act 2018 (DPA) will apply as personal information about living individuals will be being processed e.g. their movements, photographs etc.

The Information Commissioner has published a Data Protection Employment Practices Code of Practice (available at www.ico.gov.uk). Part 3 of this code covers all types of employee surveillance from video monitoring and vehicle tracking to email and internet surveillance. It gives guidance on how to do employee surveillance in a way which complies with the DPA. Whilst the code is not law, it can be taken into account by the Information Commissioner and the courts in deciding whether the DPA has been complied with.

The code states that employee monitoring should take place for a clear justified purpose and employees should be aware that it is taking place. With regard to covert surveillance it states that it will be rare for such monitoring to be justified.It should therefore only be used in exceptional circumstances e.g. prevention or detection of crime or serious malpractice. One of the other main recommendations of the code is that senior management should normally authorise any covert monitoring of employees. They should satisfy themselves that there are grounds for suspecting criminal activity or equivalent malpractice. They should carry out an impact assessment and consider whether the surveillance is necessary and proportionate to what is sought to be achieved.

The code sets out other rules that local authorities (and others) need to consider when carrying out covert surveillance of employees:

- Prior to the investigation, clear rules must be set up limiting the disclosure and access to information obtained.
- The number of people involved in a covert monitoring exercise should be limited.
- The surveillance must be strictly targeted at obtaining evidence within a set time frame and it should not continue after the investigation is complete.
- If using audio or video equipment, this should not normally be used in places such as toilets or private offices.
- Information obtained through covert monitoring should only be used for the prevention or detection of criminal activity or serious malpractice.
- Other information collected in the course of monitoring should be disregarded and, where feasible, deleted unless it reveals information that no employer could reasonably be expected to ignore.

In the above cases it is important to have a proper audit trailthrough written records. Therefore in order to demonstrate compliance the same forms for a RIPA authorisation need to be completed for a non-RIPA authorisation. The difference is that is does not need Judicial approval (no need to go to the Magistrate's Court)

NON-RIPA Authorisation Form

Application for Authorisation to conduct Covert Surveillance not regulated byRIPA

Sample Form with Notes to Assist Completion

This form should be completed by an officer of the local authority seeking authorisation to carry out surveillance which does not fall within the definition of Directed Surveillance in section 28 of the Regulation of Investigatory Powers Act 2000 (RIPA). This could include surveillance where the target is doing something which is not a criminal offence (or which does not carry a term of imprisonment of six months or more), misusing the work e-mail/internet system or breaching a legal agreement (e.g. tenancyagreement).

Before completing this form please consult*:*

- The ICO Employment Practices Code: Part 3 (Staff Surveillance)
- The Council's SRO

Once completed this form should be forwarded to your manager to complete box 11 onwards

Non-RIPA application for Authorisation Form

Organisation *(including full address)*			
Name of Applicant		**Unit/Branch /Division**	
Full Address			
Contact Details			
Investigation/Operation Name (if applicable)			
Investigating Officer (if a person other			
than the applicant)			

DETAILS OF APPLICATION
1. **Give rank or position of the authorising officer**
This is the person who will decide whether or not the surveillance should be authorised and willcountersign this form. It may be the head of the department carrying out the surveillance. If in doubt consult your legal department.
2. **Describe the purpose of the specific operation or investigation.**
Explain what is being investigated. For example: • Misuse of email/internet • An employee "fiddling" his/her timesheet • Breach of a tenancy agreement If possible, include the relevant legislation that which gives you the power/duty to investigatethe matter and to take action.

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

The key phrase is "in detail." Therefore a response which merely states **"**Video camera andrecording equipment will be installed at a fixed point" will not be adequate.

Your statement here needs to include what is going to be done, who is going to do it, whenthey are going to do it, where they are going to do it and how they are going to do it. Other points to address here include:

- How long will the surveillance last?
- Specific details about dates and times i.e. is it 24/7, at specific times of the day or atrandom times?
- Which premises are to be used and/or targeted?
- Which vehicles are to be used? Are they public or private?
- What type of equipment is to be used? e.g. covert cameras, audio devices
- What is the capability of the equipment to be used? e.g. zoom lense, remote controlledetc.
- Who else will be involved in the operation and what will be their role? e.g. privatedetectives, police

It may be appropriate to attach plans/maps showing where and how the surveillance will beconducted and indicating where any surveillance equipment will be installed.

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

- Name:
- Address:

- DOB:
- Other information as appropriate:

Include as much information as you have. If you do not know the identity of the target(s) thensay so. You could include a general description of the target(s).

5. **Explain the information that it is desired to obtain as a result of the directedsurveillance.**

Your statement here should be more detailed than in Box 2. You should give details of theprecise information sought by doing the surveillance. For example:

- "To ascertain what time the employee enters and leaves the office."
- "To capture images of the employee making unauthorised visits to service users."
- "To find out what websites the employee has been visiting and what images have beendownloaded."

6. **Has any warning/notice been served on the target? If not, explain why thissurveillance needs to be covert**
The warning could be general one (e.g. signs/policy) or it could be more specific (e.g. letter). Explain any overt methods you have tried to obtain the evidence/information or why they arenot appropriate. Explain the consequences of the target finding out about this surveillance.
7. **Explain <u>why</u> this surveillance is necessary**
Include in this box details of: • Why surveillance is needed to obtain the information/evidence that is sought • Any other means you have tried (not involving surveillance) to obtain the sameinformation/evidence • Any other evidence/information you have to link the target with the offender whichrequires corroboration through surveillance
8. **Supply details of any potential collateral intrusion and why the intrusion is unavoidable.** Describe precautions you will take to minimise collateral intrusion

(Firstly, identify which third parties will be the subject of collateral intrusion and what thatintrusion will be i.e. what information will be captured about them?

Secondly, state why this is unavoidable. This could be because of the nature of the premises (e.g. a restaurant) or because of what the person is doing (e.g. visiting the subject/target premises). In some cases there will always be third parties around who will be captured on filmor whose activities will be recorded/observed in some way.

Thirdly, set out what steps you have taken to minimise collateral intrusion, if this is possible.

If you cannot minimise collateral intrusion you still need to show you have considered it. In some situations all you may be able to state is that you cannot do anything to minimise collateral intrusion but you will not be making any decisions based upon the information gathered about third parties unless it shows them committing a criminal offence. Furthermore,you will ensure that officers who do the surveillance or view any recordings are mindful of whothe real target of the surveillance is.)

9. **Explain <u>why</u> this 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 theevidence be obtained by any other means?**

The RIPA Covert Surveillance Code of Practice contains detailed guidance on proportionality:

"3.3…This involves balancing the seriousness of the intrusion into the privacy of the target ofthe operation (or any other person who might be affected) against the need for the activity in investigative and operational terms."

" 3.4 The authorisation will not be proportionate if it is excessive in the overall circumstances ofthe case. Each action authorised should bring an expected benefit to the investigation or operation and should not be disproportionate or arbitrary. The fact that a suspected offence may be serious will not alone render intrusive actions proportionate. Similarly, an offence may be so minor that any deployment of covert techniques would be disproportionate. No activity should be considered proportionate if the information which is sought could reasonably be obtained by other less intrusive means."

Here you demonstrate that you have:

- balanced the size and scope of the proposed activity against the gravity and extent ofthe perceived crime or offence;
- explained how and why the methods to be adopted will cause the least possibleintrusion on the target and others;
- considered whether the activity is an appropriate use of the legislation and a reasonableway, having considered all reasonable alternatives, of obtaining the necessary result;
- evidenced, as far as reasonably practicable, what other methods had been consideredand why they were not implemented.

In order to comply with the above you need to address the following questions:

- Can you get information using less intrusive means/overt methods?

- What other means have you tried to obtain the same information/evidence?
- What have you done to try and lessen the impact on the target? Factors to addressinclude:

  - Amount of information to be gathered during surveillance
  - The way the surveillance is done e.g. using still cameras rather than video tocapture less information or using one camera rather than two.
  - Impact of the surveillance on the subject
  - Timing of the surveillance

At the same time, the above must be balanced with the need for the activity in operationalterms. To demonstrate this balance you should address:

- What you are seeking to achieve?
- Seriousness and extent of the offence
- Impact of the offence on the victims, others/wider community and on the public purse

For more guidance on proportionality see chapter 3 of the RIPA Covert Surveillance Code andthe Employment Practices Data Protection Code (Part 3).

10. **Applicant's Details**.			
Name (print)		**Tel No:**	
Grade/Rank		**Date**	
Signature			

11. **Authorising Officer's Statement. [Spell out the "5 W's" – 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, Who is the surveillance directed against, Where and When will it take place,What surveillance activity/equipment is sanctioned, How is it to be achieved?]*

This section is for the Authorising Officer to complete. Ensure that you are satisfied that any covert monitoring is strictly targeted at obtaining evidence within a set timeframe andthat it does not continue after the investigation is complete.

Sufficient detail must be included here to demonstrate that you, as the Authorising Officer,have considered the application objectively. Reference can be made to the boxes completed by the Investigating Officer above but "cut and paste" should be avoided. The five "W's" stated above must be addressed in detail. This is important so that the

Investigating Officers are clear as to what they can and cannot do and the means theycan adopt.

You should not be afraid to reject the application if it lacks clarity or detail.

12. **Explain <u>why</u> you believe the surveillance is necessary.**
Explain <u>why</u> you believe the surveillance to be proportionate to what is soughtto be achieved by carrying it out.

You should satisfy yourself that there are grounds for suspecting criminal activity or equivalent malpractice and that notifying individuals about the monitoring would prejudiceits prevention or detection. Set out what matters in the respective boxes you have given particular weight to when considering necessity and proportionality. You can also add anyadditional factors you have considered.

Date of first review		If the surveillance operation is going to last more than amonth then you should consider whether it should be reviewed after a period of time. During a review, consideration will have to be given to whether the surveillance is still necessary and proportionate.		
Programme for subsequent reviews of this authorisation: Only complete this box if review dates after the first review are known. If not or inappropriate to set additional review datesthen leave blank.				
Name (Print)		**Grade / Rank**	State the position of the AuthorisingOfficer e.g. Head of Audit	
Signature		**Date and time**		
Authorising Officers should not normally be responsible for authorising operations in which they are directly involved, although it is recognised that this may sometimes be unavoidable, especially in thecase of small organisations, or where it is necessary to act urgently or for security reasons.				
Expiry date and time				

10.0 Member Involvement

The Cabinet/Executive Board should consider reports on the use of the powers under the Act on a regular basis, which shall be at least every year, to ensure that it is being used consistently with this policy. Cabinet/Executive Board will also consider reports from the IPCO. Members of the Council will not however be involved in making decisions on specific authorisations.

Appendix 1

Inventory of Surveillance Equipment held by ELDC and BBC

(There is currently no surveillance equipment owned or used by either Council)

The Equipment should be stored, when not in use, in a locked cabinet under the control of the Senior Responsible Officer.

Any Officer of the Council considering using the Equipment for covert surveillance in a public place must make a written request to the Senior Responsible Officer or the RIPA coordinating Officer, who will consider and decide whether the proposed use of the Equipment is appropriate, bearing in mind the provisions of RIPA and the associated codes of practice.

Any Officer who uses the Equipment to record digital images may only view such images once captured, and shall not download them on to a computer or other electronic storage facility unless this is first agreed by the Senior Responsible Officer and/or the RIPA coordinating Officer.

Appendix 2 Social Media

Guidance on the use of Social Networking Sites for investigations

It is recognised that the use of the internet and, in particular, social networking sites, can provide useful information for Council staff carrying out investigations. These investigations may relate to the various enforcement roles within the council – for example Fraud, Planning Enforcement, Licensing or Environmental Health, but will equally apply to some non-enforcement teams, such as Debt Collection or Housing.

The use of the internet and social networking sites may fall within the definition of covert directed surveillance. This is likely to result in the breaching of an individual's Article 8 rights under the Human Rights Act (the right to privacy).

Social Networking Sites

There is a fine line between general observation, systematic observation and research and it is not sufficient to rely on a perception of a person's reasonable expectations or their ability to control their personal data.

Guidance for officers in relation to the use of social media for the gathering of evidence to assist in its enforcement activities is set out below:

- Officers must not 'friend' individuals on social networks as part of undertaking their roles
- Officer must not use their own private social networking accounts to view the social networking accounts of other individuals as part of their professional role
- Officers viewing an individual's profile on a social networking site should do so only once in order to obtain evidence to support or refute their investigation
- further viewing of open profiles on social networking sites to gather evidence or to monitor an individual's status, must only take place once RIPA authorisation has been granted and approved by a Magistrate
- Officers should be aware that it may not be possible to verify the accuracy of information on social networking sites and, if such information is to be used as evidence, steps must be taken to ensure its validity.

The **purpose** of this guidance note is to provide clarity on the Councils' position:

- It is not possible to provide a definitive list of social networking sites, so this should be taken to mean any site which involves individuals creating a profile which contains personal information and is viewable by others, whether accepted as 'friends' or otherwise.

- This might include sites such as 'Facebook' and 'LinkedIn'

- As the definition of 'private information' under RIPA includes:
  'any information relating to a person's private or family life and should be taken generally to include any aspect of a person's private or personal

relationship with others, including family and professional or business relationships'

> *The Chief Surveillance Officer says:* 'Although there remains a significant debate as to how anything made publically available in this medium can be considered private, my commissioners remain of the view that the repeat viewing of individual 'open source' sites for the purpose of intelligence gathering and data collation should be considered within the context of the protection that RIPA affords to such activity.
>
> *There is a fine line between general observation, systematic observation and research and it is unwise to rely on a perception of a person's reasonable expectations or their ability to control their personal data.'*

- Sites used to advertise goods and services should be included within the definition. Although there is likely to be a reduced expectation of privacy with this type of site, there is still the possibility of obtaining private information which may be subsequently used in any enforcement proceedings.
- If an allegation is received or, as part of an investigation into an individual, it is necessary to view their social networking site, officers may access the main page of the individual's profile **once** in order to take an initial view as to whether there is any substance to the allegation or matter being investigated.
- The initial viewing must be reasonable – for example, it would not be reasonable to spend any significant amount of time searching through various pages of the individual's profile or to print out several pages just in case they may reveal something useful.
- In some cases where, for example, a link to a site is provided by a complainant, it may be relevant for the receiving officer to view the link before passing it onto the investigating officer to also view. This would count as one viewing.
- However, it would not be reasonable for each officer in a team to view the site in turn so that they may each gather some information.
- Each single viewing of an individual's social networking site must be recorded on the investigation file stating who viewed it, when and why. This is to enable scrutiny and reporting to IPCO if necessary as well as to evidence on the investigation file that there has been no misuse of RIPA.
- If it is considered that there is a need to further monitor an individual's social networking site with a view to gathering evidence then authorisation must be obtained from an Authorising Officer.
- If the offence being investigated falls under RIPA, a formal RIPA application must be completed, authorised by one of the Councils' Authorising Officers and then approved by a Magistrate.
- If the offence being investigated falls outside of RIPA (for example if the offence does not carry a custodial sentence of at least 6 months imprisonment or is not a core function of the council) a non-RIPA form must be completed General guidance on RIPA and appropriate forms can be found on the Councils' Intranet and in the main RIPA Policy document

Appendix 3

List of Officers Authorised under this Policy:

NAME	POSITION	CONTACT
Christian Allen	Senior Responsible Officer and RIPA Coordinator	
Duncan Hollingworth	Authorising Officer	
Andy Fisher	Authorising Officer	
Peter Hunn	Non-RIPA Authorising Officer	
Matt Fisher	Non-RIPA Authorising Officer	

Appendix 4

GRANTING OF AUTHORISATION FOR THE USE OF COVERT HUMAN INTELLIGENCE SOURCES (CHIS) *Not usually used by Councils*

The same requirements of necessity and proportionality exist for the granting of these authorisations as with directed surveillance.

Additionally, the Authorising Officer shall not grant an authorisation unless he /she believes that arrangements exist which satisfy the following requirements:

- there will at all times be an officer with day to day responsibility for dealing with the source and the source's security and welfare
- there will at all times be an officer who will have general oversight of the use made of the source
- there will at all times be an officer with responsibility for maintaining a record of the information supplied by the source
- records which disclose the identity of the source will not be available to persons except to the extent that there is a need for access to them to be made available

Similarly, before authorising the use or conduct of the source, the Authorising Officer must be satisfied that the conduct/use is proportionate to what the use or conduct of the source seeks to achieve, taking into account the likely degree of intrusion into the privacy of those potentially effected, and for the privacy of persons other than those who are directly the subjects of the operation or investigation.

Measures should be taken, wherever practicable, to avoid unnecessary intrusion into the lives of those not directly connected with the operation.

- Particular care is required where people would expect a high degree of privacy, or where, as a consequence of the authorisation, 'confidential material' is likely to be obtained.
- Consideration is also required to be given to any adverse impact on community confidence that may result from the use or conduct of a source or information, obtained from that source.
- Additionally, the Authorising Officer should make an assessment of any risk to a source, in carrying out the conduct in the proposed authorisation.
- Authorisation for the use of a CHIS must be given in writing.

Only the Chief Executive (or in his/her absence the person who is formally nominated to act as the Chief Executive) may authorise the use of a juvenile or vulnerable CHIS.

Ideally, the Authorising Officers should not be responsible for authorising their own activities e.g. those in which they themselves are to act as a source, or in tasking a source. However, it is recognised that this will not always be possible, especially in the case of small departments. Authorisations must be approved by a Magistrate (see paragraph 7.5).

The Solicitor employed by the Council will arrange the appointment before the Magistrate(s) and explain the procedure to the Authorising Officer. The Solicitor employed by the Council and the Authorising Officer will be required to attend before the Magistrate(s) to seek the Magistrate's approval to the authorisation.

An **application** for authorisation for the use or conduct of a CHIS will be made on the appropriate form and must record:

1. Details of the purpose for which the source will be tasked, or deployed.

2. The reasons why the authorisation is necessary in the particular case and the grounds on which authorisation is sought (e.g. for the purpose of preventing or detecting crime or disorder).

- Where a specific investigation or operation is involved, details of that investigation or operation.

- Details of what the source would be tasked to do.

- Details of potential collateral intrusion and why the intrusion is justified.

- Details of any confidential material that might be obtained as a consequence of the authorisation.

- The reasons why the authorisation is considered proportionate to what it seeks to achieve.

- The level of authorisation required.

- A subsequent record of whether authorisation was given or refused by whom and the time and date.

Duration of Authorisation of a CHIS

A written authorisation, unless renewed, will cease to have effect at the end of a period of twelve months beginning with the day on which it took effect except in the case of a juvenile CHIS which has a duration of one month. Oral authorisations will, unless renewed, last 72 hours.

Renewal of a CHIS

As with authorisations for directed surveillance, authorisations for the conduct and use of CHIS can be renewed, the same criteria applying. However before an Authorising Officer renews an authorisation, he must be satisfied that a review has been carried out of the use of a CHIS and that the results of the review have been considered.

Applications for renewal must be made on the appropriate form and submitted to the Authorising Officer. However, an application for renewal should not be made until shortly before the authorisation period is coming to an end.

An authorisation may be renewed more than once provided it continues to meet the criteria for authorisation.

When CHIS authorisation requires renewal, the renewal must be approved by a magistrates' court in the same manner as an initial authorisation

Review

Regular reviews of authorisations should be undertaken. The results of the review should be recorded on the appropriate form and a copy filed on the central record of authorisations.

If the surveillance provides access to confidential information, or involves collateral intrusion, frequent reviews will be required. The Authorising Officer should determine how often a review should take place.

- Before an Authorising Officer renews an authorisation he must be satisfied that a review has been carried out of:
- The use made of the source during the period authorised
- The tasks given to the source
- The information obtained from the use or conduct of the source
- If the Authorising Officer is satisfied that the criteria necessary for the initial authorisation continue to be met, he may renew it in writing as required.

When CHIS authorisation requires renewal, the renewal must be approved by a magistrates' court in the same manner as an initial authorisation

Cancellations

The officer who granted or renewed the authorisation **MUST** cancel it if he/she is satisfied that

- the use or conduct of the source no longer satisfies the criteria for authorisation, or
- that the arrangements for the source's case no longer exist
- Requests for cancellation will be made on the appropriate form and submitted to the Authorising Officer for authorisation of the cancellation.

All CHIS cancellations must include directions for the management and storage of any surveillance product.