APPENDIX 1

REGULATION OF INVESTIGATORY POWERS ACT 2000

POLICY & PROCEDURAL GUIDANCE ON THE USE OF COVERT SURVEILLANCE

MALDON DISTRICT COUNCIL

APPENDIX 1

1. Introduction

Context

1.1. This document sets out the Council's approach to ensure-

1.2. Council Investigations are conducted in accordance with the requirements of the Regulation of Investigatory Powers Act 2000 (RIPA) and guidance issued by the various statutory agencies, specifically the Home Office Code of Practice for Covert Surveillance and Property Interference at:

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

i) The Council can justify the need for covert investigation techniques, which by their very nature may otherwise be in breach of the Human Rights Act 1998, and that appropriate controls are in place to ensure that the activities are properly controlled and monitored.

Why is RIPA important?

1.3. The provisions of RIPA are designed to regulate any act of covert investigation or surveillance carried out by a local authority. These terms are explained below.

1.4. RIPA was enacted to provide a lawful procedure for public bodies to carry out covert investigations without the risk of a claim being made under the Human Rights Act 1998, against either that body or the Investigating Officer, by the person subject to such an investigation.

1.5. The Human Rights Act introduced a remedy for persons claiming that their privacy had been breached. The right to privacy contained in the European Convention on Human Rights (ECHR) is not an absolute right. It is a qualified right and will not apply in the circumstances set out in Article 8.2 of the ECHR.

1.6. The provisions of Article 8.2 of the ECHR have been incorporated into English law by the enactment of Part II of RIPA. The effect of Part II of RIPA is to provide protection to the local authority itself and to the individual officer against any claim for breach of privacy, provided they can demonstrate that they have fully complied with the procedures prescribed by RIPA.

1.7. If an investigation is carried out in accordance with RIPA procedures, then any possible resultant breach of the subject's privacy rights would not be actionable as a civil claim. In addition, in criminal proceedings arising from the investigation, the evidence gathered will not be challengeable under Section 78 of the Police & Criminal Evidence Act 1984, on the ground that it is a breach of privacy rights.

1.8. The protection afforded by RIPA also extends to complaints made to the Investigatory Powers Tribunal and to the Local Government Ombudsman. Strict

adherence to the requirements of RIPA therefore provides a defence to any civil proceedings and claims for damages for breach of privacy.

1.9. It is therefore crucial that all Investigating Officers adhere to the requirements of RIPA.

What RIPA Does and Does Not Do

1.9 RIPA does:

i) Require prior authorisation of directed surveillance;

ii) Prohibit the Council from carrying out intrusive surveillance;

iii) Require authorisation of the conduct and use of a Covert Human Intelligence Source (CHIS); and

iv) Require safeguards for the conduct and use of a CHIS.

1.10 RIPA does not:

i) Make conduct unlawful which would otherwise be lawful; and

ii) 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.

2. Scope of the RIPA Investigation process

Reason for the Guidance

2.1 This policy is intended to assist any employee of the Council who acts as an Enforcement (Investigating) Officer in any capacity or who acts as an Authorising Officer. It will direct officers from the start of the investigation to the point at which the legal process will begin which is beyond the scope of this guidance. It does not replace the need for proper training in investigation techniques.

2.2 If the Authorising Officer or any Applicant is in any doubt, s/he should ask the Authorising Officer or BEFORE any directed surveillance and/or CHIS is authorised, renewed, cancelled or rejected.

Training

2.3 The RIPA Co-ordinating Officer will ensure refresher training for those officers whose work involves, or is likely to involve, the use of the RIPA regime every 12 months.

The RIPA Co-ordinator has responsibility for arranging training for Authorising Officers with respect to Covert Human Intelligence Sources "CHIS" and for raising awareness more generally among staff with investigative roles.

2.4 New members of staff for whom the above is applicable should access the RIPA on-line "Act Now" training module once approved by their manager (https://www.actnow.org.uk/ripaessentials). Human Resources maintain records of formal RIPA training.

2.5 There should be regular updates at team meetings on the use of RIPA. Guidance with respect to Covert Human Intelligence Sources is available both on the intranet and from the RIPA Co-ordinating officer.

Home Office Guidance

2.6 The Home Office provides guidance on the use by public authorities of RIPA legislation in its Code of Practice. It is important that officers involved with RIPA are familiar with this code, particularly Authorising Officers as public authorities may be required to justify, with regard to the code, the use or granting of authorisations in general or the failure to use or grant authorisations where appropriate.

3. Meaning of Surveillance

3.1 RIPA provides for the authorisation of covert surveillance by public authorities, where the surveillance is likely to result in the obtaining of private information about a person. It does so by establishing a procedure for authorising covert surveillance. It prescribes the office, rank and position of those permitted to authorise covert surveillance. From 1st November 2012 any authorisation cannot be granted by a local authority unless it is first approved by the Magistrates' Court.

What is Surveillance?

3.2 Surveillance includes:-

i) Monitoring, observing or listening to persons, their movements, their conversations or any of their activities or communications

ii) Recording anything monitored, observed or listened to in the course of surveillance

iii) Surveillance by or with the assistance of any surveillance device.

Examples of Different Types of Surveillance:

Type of Surveillance	Examples
Overt Eg Officers on patrol (community engagement officers/environmental health officers)	• Signposted Town Centre CCTV cameras (in normal use) • Recording noise coming from outside the premises after the occupier has been warned that this will occur if the noise persists.
Covert but do not require prior authorisation	• CCTV cameras providing general traffic, crime or public safety information • Most test purchases where the officer does not identify themselves upon entry and views activity as if they are a member of the public.
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.

What is Overt Surveillance?

3.3 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 will be behaving in the same way as a normal member of the public and/or will be going about Council business openly.

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

What is Covert Surveillance?

3.5 Covert Surveillance is any surveillance which is carried out in a manner calculated to ensure that the subject is unaware it is or may be taking place. The provisions of RIPA authorise the following forms of covert surveillance:

i) Directed surveillance;

ii) Intrusive surveillance; and

iii) The conduct and use of covert human intelligence sources (CHIS).

3.6 RIPA does not enable a local authority to make any authorisations to carry out intrusive surveillance. This type of surveillance is considered in more detail in paragraphs 3.11- to 3.15 below

What Is Directed Surveillance?

Local authorities are permitted under RIPA to authorise directed covert surveillance on the grounds that such surveillance is necessary for the prevention or detection of crime. Surveillance is directed if it is covert but not intrusive and is undertaken:

i) For the purpose of a specific investigation or a specific operation;

ii) In such a manner as is likely to result in the obtaining of private information about a person (whether or not one specifically identified for the purposes of the investigation or operation); and

iii) Otherwise, and by way of an immediate response to events or circumstances the nature of which is such that it would not be reasonably practicable for an authorisation under RIPA to be sought for the carrying out of the surveillance.

Limitations on the Use of Directed Covert Surveillance

3.7 The Regulation of Investigatory Powers (Directed Surveillance and Covert Human Intelligence Sources) (Amendment) Order 2012 (SI 2012/1500) (2012 Order) came into force on 1 November 2012. It restricts Authorising Officers in a local authority in England or Wales, from authorising the carrying out of directed surveillance unless it is for the purpose of preventing or detecting a serious criminal offence or for preventing public disorder and meets the following conditions:

i) That the criminal offence to be prevented or detected is punishable by a maximum term of at least six months' imprisonment; or

ii) It constitutes an offence under sections 146, 147 or 147A of Licensing Act 2003 (sale of alcohol to children) or section 7 of the Children and Young Persons Act 1933 (sale of tobacco to children under 18 years old).

iii) In the case of preventing public disorder, if it involves a criminal offence punishable by a maximum term of six months.

3.8 It is therefore essential that Investigating Officers consider the penalty attached to the criminal offence which they are investigating, before considering whether it may be possible to obtain an authorisation for directed surveillance. The maximum sentence should be indicated on the RIPA application form.

3.9 In addition, Intrusive Surveillance cannot be authorised for use by the Council.

What is Intrusive Surveillance?

3.10 This is surveillance which is covert surveillance that:

i) Is carried out in relation to anything taking place in any residential premises or any private vehicle; and

ii) Involves the presence of an individual on the premises or in the vehicle or is carried out by means of a surveillance device.

3.11 Residential premises include a rental flat occupied for residential purposes, a police cell and a hotel bedroom. However, examples of places which may not be regarded as residential premises are a communal stairway in a block of flats or the front garden of premises readily visible to the public.

3.12 Therefore, it is important to note that not all surveillance of a suspect's home or vehicle is likely to amount to intrusive surveillance. For example, if an Investigating Officer observes a suspect leaving his home from the street using binoculars, this is unlikely to be intrusive, unless the quality of the image obtained is of the same quality as might be expected to be obtained from a device actually present on the premises.

3.13 There are also a number of exceptions applicable to the use of certain monitoring equipment some of which are not considered to constitute the use of intrusive surveillance. But the intrusiveness of the surveillance proposed must be considered before any surveillance operation takes place. Therefore, advice should be sought in advance before such surveillance is contemplated or it may not be admissible as evidence and may also be a breach of RIPA.

3.14 For the avoidance of doubt, surveillance that enables an Investigating Officer to view or monitor anything going on inside a dwelling is almost certainly going to be regarded as intrusive and conduct of that nature cannot be authorised by a local authority.

What is Private Information and why is this Important?

3.15 Information is considered to be private information if it includes any information relating to the subject's private or family life or the private or family life of any other person. It would include any aspect of a person's private or personal relationship with others, including family and professional or business relationships. Private information may include personal data for example names, telephone numbers and address details.

3.16 It is important to understand this as Enforcement Officers may obtain information of this nature as part of an investigation for which a RIPA authorisation is not needed. However, if officers as part of that investigation obtained private information, a RIPA authorisation would be required to use it.

3.17 For example, if Enforcement Officers photographed the exterior of business premises, this in itself would not amount to surveillance requiring a RIPA authorisation. However, if officers also wanted to establish a pattern of occupancy of those premises by any person and took photographs on a number of occasions, it is likely that private information would be obtained and therefore a RIPA authorisation would be required. Care is therefore needed in deciding the ultimate purpose of the surveillance and what evidence officers are seeking to capture.

3.18 Private information may also be acquired through covert surveillance even where a person is in a public place and may have a reduced expectation of privacy. For example, where two people hold a conversation on the street they may have a reasonable expectation of privacy over the contents of that conversation. A directed surveillance authorisation may therefore be required if a public authority records or listens to the conversation as part of a specific investigation or operation.

3.19 In addition, the totality of the information relating to the private life of an individual may constitute private information, even if the individual records do not, and in this case an authorisation is required. For example where-

i) A number of records are analysed together; or

ii) A number of pieces of information are obtained, covertly, for the purpose of making a record about a person or for data processing to generate further information.

4. When is a RIPA Authorisation required?

4.1 As explained in section 1 of this guidance, interference with any individual's rights under the HRA is a statutory offence. Whilst the provisions of RIPA provide lawful reasons to do so officers need to be aware that they need to assess in all cases if their surveillance or other actions might breach any of the HRA rights.

4.2 Officers must assess whether an individual's human rights may be breached and provide justification for doing so based on the relevant tests in the HRA. For example, surveillance that falls into the following categories will not be covered by RIPA:

(i) Crimes not carrying six months imprisonment

(ii) Employee Surveillance

4.3 In addition some surveillance activity does not constitute directed surveillance at all for the purposes of RIPA and no authorisation can be provided for such activity under that act. These activities include:

i) Covert surveillance by way of an immediate response to events;

ii) Covert surveillance as part of general observation activities;

iii) Covert surveillance not relating to the prevention or detection of crime or the prevention of disorder; and

iv) Overt surveillance by CCTV.

4.4 For example, enforcement officers attending a market where it is suspected that counterfeit goods are being sold, may not be carrying out surveillance of any particular individual as their intention is to identify and tackle offenders generally. In these circumstances this forms part of the general duties of the public authority and the obtaining of private information is unlikely. In such a case a directed surveillance authorisation is not required, but an assessment of any interference under the HRA is still necessary.

4.5 Covert surveillance undertaken without a RIPA authorisation will not have the protection of RIPA but 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 HRA. Article 8 of the ECHR states:

"everyone has the right to respect for his private and family life his home and his correspondence; **and**

There shall be no interference by a public authority with the exercise of this right except such as is 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"

4.6 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.

4.7 It is just as important to have a written record of non-RIPA authorisation. Accordingly, officers who wish to undertake any surveillance must complete a RIPA authorisation form. This must then be passed to an authorising officer who will consider whether or not to authorise it as non-RIPA surveillance or advise that RIPA applies. The process for seeking this authorisation is set out in Section 5A below.

CCTV Systems

4.8 Where overt surveillance equipment is used for example in town centres, members of the public will be aware of their use and no RIPA authorisation is required.

4.9 If, however, CCTV cameras are used in a covert, pre-planned manner as part of a specific investigation or operation for the surveillance of a particular individual, then an authorisation for directed surveillance may be required. Such surveillance is likely to result in the obtaining of private information about a person, that is, a record of his movements and activities.

An Example of the Use of Directed Surveillance

4.10 This type of surveillance may be used to gather evidence for an offence such as a breach of the Trade Marks Act 1994. An Investigating Officer may need to carry out surveillance of a suspect's home to obtain information about their contacts and work patterns.

4.11 This would be directed surveillance as it would result in obtaining private information. A RIPA authorisation should be obtained. The Investigating Officer would need to demonstrate that such surveillance was necessary and proportionate. The Authorising Officer must be satisfied that the action proposed would not amount to intrusive surveillance, and place conditions on the conduct to avoid this happening prior to authorising the application or decline to authorise as necessary.

4.12 Note that if the surveillance involves the use of a surveillance device, that provides detail of the same quality as may be expected to be obtained by a device located on the premises, this may amount to intrusive surveillance. No RIPA authorisation may be given for intrusive surveillance.

Grounds for Making an Authorisation under RIPA

4.13 The grounds on which a local authority may make an authorisation permitting the use of directed surveillance under RIPA are limited to the prevention or detection of serious crime or the prevention of disorder. If directed surveillance is carried

out for any other purpose, then an authorisation under RIPA cannot be granted.

Core Functions

4.14 The Council can only make authorisations under RIPA when performing its core functions. Those are the specific public functions undertaken by the local authority as opposed to its ordinary functions which are undertaken by all public authorities.

4.15 For example, an authorisation under RIPA cannot be used when the principal purpose of an investigation is for taking disciplinary action against an employee, as the disciplining of an employee is not a core function. It may, however, be appropriate to seek an authorisation under RIPA if there are associated criminal investigations.

The Conduct of Covert Human Intelligence Sources

4.16 A local authority may grant an authorisation under RIPA for the use of a covert human intelligence source (a "CHIS".) The City Council had decided as a matter of policy not to undertake this type of surveillance but it is now accepted that RIPA should only be authorised in exceptional circumstances and only after the Authorising Officer has agreed this with the RIPA Senior Responsible Officer (SRO).

4.17 A person is considered to be a CHIS if:

i) They establish or maintain a personal or other relationship with a person for the covert purpose of doing anything falling within paragraphs (ii) or (iii) below;

ii) They covertly use such a relationship to obtain information or provide access to any information to another person;

iii) They covertly disclose information obtained by the use of the said relationship, or as a consequence of the existence of such a relationship.

4.18 The type of conduct that could be authorised is any that:

i) Is comprised in any such activity including the conduct of CHIS or use of CHIS, as are specified in the authorisation;

ii) Consists in conduct by or in relation to a person who is so specified or described as a person as to whose actions as a CHIS the authorisation relates;

iii) Is carried out for the purposes of or in connection with the investigation or operation so specified or described; and

iv) Is necessary and proportionate to the intelligence dividend that it seeks to achieve.

Management of Covert Human Intelligence Sources

4.19 As indicated, it is the Council's policy to only use CHIS in exceptional

circumstances. In adopting this policy the Council recognises that there may be occasions when obtaining information by use of a CHIS is required.

4.20 Should an Investigating Officer believe that a CHIS should be used, an initial discussion should be conducted with an appropriate Authorising Officer who, if in agreement, will discuss the matter with the Senior Responsible Officer.

4.21 In deciding whether the use of a CHIS is appropriate, due regard will be had for the Home Office CHIS Code of Practice which all officers involved in the use of CHIS should be familiar with, and the relevant RIPA legislation.

4.22 It is important that all aspects of CHIS takes account of and complies with the Code of Practice:

https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/742042/20180802_CHIS_code_.pdf

The Acquisition of Communications Data

4.23 Before considering submitting an application for the acquisition of communications data, all officers must first refer the matter to the Senior Responsible Officer or the RIPA Co-Ordinating Officer

4.24 Communications Data ('CD') is the 'who', 'when' and 'where' of a communication, but not the 'what' (i.e. the content of what was said or written). Local Authorities are not permitted to intercept the content of any person's communications.

4.25 Part 3 of the Investigatory Powers Act 2016 replaced Part 1 Chapter 2 of RIPA in relation to the acquisition of communications data and puts local authorities on the same standing as the police and law enforcement agencies. Previously local authorities have been limited to obtaining subscriber details (known now as "entity" data) such as the registered user of a telephone number or email address. Under the Investigatory Powers Act 2016, local authorities can now also obtain details of in and out call data, and cell site location. This information identifies who a criminal suspect is in communication with and whereabouts the suspect was when they made or received a call, or the location from which they were using an Internet service. This additional data is defined as "events" data.

4.26 A new threshold for which "events" data can be sought has been introduced under the Investigatory Powers Act as "applicable crime". Defined in section 86(2A) of the Act this means: an offence for which an adult is capable of being sentenced to one year or more in prison; any offence involving violence, resulting in substantial financial gain or involving conduct by a large group of persons in pursuit of a common goal; any offence committed by a body corporate; any offence which involves the sending of a communication or a breach of privacy; or an offence which involves, as an integral part of it, or the sending of a communication or breach of a person's privacy. Further guidance can be found in paragraphs 3.3 to 3.13 of CD

Code of Practice.

https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/757850/Communications_Data_Code_of_Practice.pdf

4.27 The Investigatory Powers Act has also removed the necessity for local authorities to seek the endorsement of a Justice of the Peace when seeking to acquire communications data. All such applications must now be processed through NAFN and will be considered for approval by the independent Office of Communication Data Authorisation (OCDA). The transfer of applications between local authorities, NAFN and OCDA is all conducted electronically and will therefore reduce what can be a protracted process of securing an appearance before a Magistrate or District Judge (see local authority procedures set out in paragraphs 8.1 to 8.7 of the CD Code of Practice).

"DP's" To be a DP for the purposes of a Local Authority an individual must be either a Director, Head of Service, or Service Manager or equivalent. At Maldon District Council these are Richard Holmes, Director of Service Delivery and Head of Paid Service, Emma Holmes, Senior Legal Specialist and Data Protection Officer, and Grant Hulley, Lead ICT Specialist and Senior Information Risk Manager.

Maldon District Council is a member of National Anti – Fraud Network (NAFN) and all applications for data communications are made to this organisation which acts as the Council's Single Point of Contact (SPOC) and "gate keepers" ensuring that all applications are reviewed for legal compliance prior to being submitted for approval to the Council's DP.

All the appropriate forms are available on the NAFN website which also provides guidance for their completion at:-

http://www.nafn.gov.uk

5.The Procedure for Obtaining Authorisations- Directed Surveillance

5.1 Each form of covert surveillance subject to RIPA must be authorised in accordance with the provisions of RIPA.

5.2 Regulations prescribe that within a local authority, Authorising Officers must hold the rank of Director, Head of Service, Service Manager or equivalent (eg Lead Specialist). The following post holders are designated as Authorising Officers.

5.3 The officers appointed by the District Council are-

i) Director of Service Delivery

ii) Senior Legal Specialist (DPO)

iii) Lead ICT Specialist (SIRO)

iv) Lead Specialist Community

v) Resources Specialist Service Manager

vi) Community Safety Manager

Making an Application for an Authorisation

5.4 The Council is also required to have a designated RIPA Senior Responsible Officer who has primary responsibility for the integrity of the RIPA scheme and is responsible for the administration of the policy and procedures. At the District Council this is the Community Safety Manager.

5.5 The Investigating Officer must complete all the information required by the appropriate prescribed form.

5.6 The forms, guidance for completing the forms and the RIPA manual can be found on Fresh Service here -

5.7 The Investigating Officer must obtain a unique reference number for the form from the RIPA Co-ordinating Officer and must note it on the appropriate form. The form must also include:

i) Precisely what type of surveillance is to be authorised and against which subjects, the property or location and the techniques and equipment to be used and the maximum penalty applicable for the offence to be investigated;

ii) The reason why the directed surveillance is necessary i.e. it is needed for the detection or prevention of crime or disorder and why it is necessary for the investigation of this specific case;

iii) Officers should, particularly, indicate on the application form the offences relied upon to found necessity;

iv) The reason why it is considered that the use of the surveillance requested is proportionate to the objective to be achieved i.e. what is sought to be achieved by carrying out the covert surveillance and why that objective cannot be achieved through any other means- see below;

v) How collateral intrusion (interference with the privacy rights of others not subject to the surveillance) will be minimised;

vi) Where collateral intrusion is unavoidable, a risk assessment should be carried out and a mechanism put in place to disregard any information not relevant to the case;

vii) That any local community conditions or sensitivities have been considered; and

viii) The form should be completed electronically but if necessary may be handwritten.

Submitting the Application for an Authorisation

5.8 The Authorisation form must be submitted in writing to the appropriate Authorising Officer and signed by the Authorising Officer, in all but the most urgent cases.

Responsibilities of the AuthorisingOfficer

5.9 The Authorising Officer must ascertain that the Investigating Officer has completed all relevant sections of the appropriate authorisation form. S/He must also be satisfied that all of the matters detailed in the paragraph headed "Making an Application" above, have been properly considered and set out in sufficient detail on the form.

5.10 In particular, the Authorising Officer must be satisfied that the surveillance proposed may infringe the human rights of its subject or of others. S/He must also be satisfied that the covert surveillance for which the authorisation is sought is proportionate i.e. that the information could not be obtained by any other means and that it is necessary to further the objectives of the investigation. S/He should consider whether the benefits of obtaining the information are significant rather than marginal. S/He must also consider the risk of collateral intrusion into the privacy of other persons.

5.11 The Authorising Officer should clearly set out what activity and surveillance equipment is authorised so that the investigating Officer is certain what has been sanctioned.

5.12 If the Authorising Officer is not completely satisfied that the form has been properly completed, s/he should liaise with the Investigating Officer to obtain further information.

5.13 The Authorising Officer must also determine if the activity requires authorisation under RIPA at all. If not they will nevertheless:

i) Assess whether the activity should be sanctioned;

ii) Complete the HRA assessment and the mark the application form as non-RIPA and whether approved; and

iii) Indicate on the form whether interference with the human rights of the individual is accepted or not and the reasons why and clearly mark the form as non-RIPA using a watermark where appropriate.

Necessity and Proportionality

5.14 The 2000 Act stipulates that the person granting an authorisation or warrant for directed or intrusive surveillance, or interference with property, must believe that the activities to be authorised are necessary on one or more statutory grounds.

5.15 If the activities are deemed necessary on one or more of the statutory grounds, the person granting the authorisation or warrant must also believe that they are proportionate to what is sought to be achieved by carrying them out. This involves balancing the seriousness of the intrusion into the privacy of the subject of the operation (or any other person who may be affected) against the need for the activity in investigative and operational terms.

5.16 The authorisation will not be proportionate if it is excessive in the overall circumstances of the 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.

5.17 The following elements of proportionality should therefore be considered:

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

ii) Explaining how and why the methods to be adopted will cause the least possible intrusion on the target and others;

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

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

Avoiding Common Mistakes in RIPA Forms

5.18 Investigating and Authorising Officers can avoid making common mistakes when completing RIPA forms by referring to page 37 of the Covert Surveillance Policy and Procedures Toolkit available on FreshService at

Obtaining Court Approval for Authorisations

5.19 Authorising Officers must when making authorisations be aware that each authorisation (or renewal of an authorisation) will be subject to court approval. The Protection of Freedoms Act 2012 amends RIPA, to require that where an Authorising Officer has granted an authorisation for the use of directed surveillance or for the use of covert human intelligence sources, court approval will be required. The Authority will be required to make an application, without giving notice, to the Magistrates' Court. The Magistrates will give approval if, at the date of the grant of authorisation or renewal of an existing authorisation, they are satisfied that:

i) There were reasonable grounds for believing that obtaining the covert surveillance or use of a human covert intelligence source was reasonable and proportionate and that these grounds still remain.

ii) The "relevant conditions" were satisfied in relation to the authorisation.

iii) Relevant conditions include that:

a. The relevant person was designated as an Authorising Officer.

b. It was reasonable and proportionate to believe that using covert surveillance or a covert human intelligence source was necessary and that the relevant conditions have been complied with.

c. The grant or renewal of any authorisation or notice was not in breach of any restrictions imposed under section 25(3) of RIPA.

d. Any other conditions provided for by an order made by the Secretary of State were satisfied.

5.20 Once the application form has been signed by the authorising officer it should be passed to the RIPA Co-ordinating Officer who will ensure that the application is RIPA compliant

5.21 If RIPA compliance is satisfactory the Co-ordinating Officer will liaise with the court and the Investigating Officer to obtain a date and time on which the application can be heard.

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

5.23 No activity permitted by the authorisation granted by the Authorising Officer may be undertaken until the Magistrates' Court has approved its use.

5.24 Authorising Officers should be aware that they may be required to attend court with the Investigating Officer in order to support the application for authorisation.

5.25 The Co-ordinating Officer will usually attend court with the Investigating Officer in order to provide legal assistance if required.

Expiry of Authorisations

5.26 Written authorisations under RIPA cease to have effect 3 months after the authorisation by the court unless renewed (12 months for applications under CHIS). The three-month authorisation is mandatory and cannot be restricted. The Authorising Officer must ensure that the correct expiry date is recorded on the authorisation form. For example, an authorisation given on 1st April will expire on 30th June. Authorisations cease at 23:59 on the last day, so it is not necessary to specify a time.

Review of Authorisations

5.27 Regular reviews of authorisations which have been granted should be undertaken by the Investigating Officer to ascertain whether it is necessary for the authorisation to continue. Authorisations may be renewed at any time by any person who would be entitled to grant a new authorisation in the same terms.

Obligations of the Authorising Officer Relating to the Renewal of Authorisations

5.28 When considering an application for renewal of an authorisation the Authorising Officer must consider whether surveillance is still necessary and proportionate.

5.29 Renewals become effective on the day on which the existing authorisation expires. Renewals of authorisations will also be subject to approval by the Magistrates' Court and the Authorising Officer must provide the RIPA Co-ordinating Officer with the appropriate forms in good time to obtain a renewal if that is required.

Cancellation of Authorisations

5.30 Authorisations under RIPA do not lapse automatically. They continue for the statutory 3 month's period from the date on which the court gives authorisation, unless cancelled earlier. Once an investigation has been completed or the circumstances of the case dictate that it must be closed, the Investigating Officer must complete a cancellation of authorisation form and submit it to the Authorising Officer who granted or last renewed the authorisation.

5.31 Even if an authorisation has expired it must still be cancelled.

5.32 The Authorising Officer may cancel the authorisation if he considers that the requirements of the authorisation are no longer satisfied.

5.33 All of the information relating to the authorisation will form part of the records of the investigation and must be kept on the appropriate file for 5 years or longer if appeals are made.

5.34 Information that may be of value in connection with concurrent investigations may be kept, but information not relevant to those enquiries must be destroyed.

Maintaining Records of Authorisations, Renewals and Cancellations

5.35 The Authorising Officer must send the originals of all records of authorisations, renewals and cancellations to the RIPA Senior Responsible Officer who will keep a central record.

i) The Authorising Officer should diarise the dates for review of each authorisation; and

ii) Review the authorisations / renewals made on a regular basis to ensure that such authorisations/renewals are made properly, are appropriate and that all forms have been fully completed.

5.36 The Investigating Officer should keep the following record and diarise the dates for renewal and cancellation:

i) A copy of the authorisation together with supporting documents and specifically any Court Order approving the use of the authorisation;

ii) A copy of any renewal of any authorisation together with supporting documents;

iii) Any authorisation which was granted or renewed orally (an urgent case) and the reason why the case was considered to be urgent ;

iv) A record of the results of any reviews of the authorisation;

v) The reasons for not renewing an authorisation;

vi) The reasons for cancelling an authorisation; and

vii) The Investigating Officer should diarise the dates for review of each authorisation.

Role of the RIPA Senior Responsible Officer

5.37 In accordance with the Home Office Code of Conduct the Council designates a Senior Responsible Officer in relation to RIPA powers and delegations. The SRO

has overarching responsibility for the RIPA scheme, and in particular:

i) To ensure the integrity of the process to authorise directed surveillance, compliance with the Act and the Codes of Practice;

ii) To engage with the Commissioners and Inspectors when they conduct inspections, to oversee the implementation of any post-inspection action plan recommended or approved by an inspector;

iii) To review the operation of RIPA and report to the Governance Committee on a quarterly basis to ensure that the scheme is being used in accordance with the Council's policy and to provide statistical information with respect it's use.

iv) To prepare and submit an annual report to the Governance Committee in order for the Committee to ensure RIPA policy; remains " fit for purpose".

v) To convene a meeting with the RIPA administrative personnel every six months to review its operation.

Role of the RIPA Co-Ordinating Officer

5.38 The RIPA Co-Ordinating Officer will be the litigation lawyer who has primary responsibility for criminal litigation, and will exercise the following delegated responsibilities:

i) To ensure that a central record of all RIPA authorisations, renewals and cancellations are maintained. That paperwork is renewed prior to RIPA applications being made to the Magistrates' Court and ensure that all renewals and cancellations are RIPA compliant;

ii) To regularly review the RIPA scheme to ensure that it is compliant with the Act and the Codes of Practice;

iii) To be the legal advisor with respect to RIPA and ensure day to day compliance with the requirements of this policy ;

iv) To provide advice to Investigating and Authorising Officers; and

v) To review training requirements every 18 months and ensure that, where appropriate, training is undertaken.

vi) Provide a Unique Reference Number for each RIPA application upon request by an Investigating Officer; and

vii) Maintain a central record of all RIPA authorisations, renewals and cancellations.

Regulation of Use of Authorisations

5.39 The Investigatory Powers Commissioner reviews the exercise and performance of the use of authorisations by public bodies. Information must be provided on

request to enable the inspections that will be carried out regularly by the Surveillance Commissioner.

5.40 A tribunal has been established to consider and determine complaints relating to the exercise of RIPA powers by any person aggrieved. The tribunal deals with these matters in a similar manner to the courts when dealing with judicial review cases. Complaints must be lodged with the tribunal within one year unless the tribunal determines it is just and equitable to extend that period.

5.41 The tribunal may order the quashing or cancellation of any authorisation, records or information obtained by use of an authorisation.

5.42 The Council is under a duty to disclose to the tribunal all documents that may be required relating to the authorisation.

6. Further Information and how to make a complaint

6.1 Further information is available from:

- The Regulation of Investigatory Powers Act 2000
- RIPA Explanatory Notes
- RIPA Statutory Codes of Practice:
  a. Covert Surveillance and Property interference – see para 1.2 of this policy
  b. Covert Human Intelligence Sources – see para 4.22 of this policy
  c. Acquisition and Disclosure of Communications Data – see para 4.26 of this policy
- SI 2000 No.20793 The Regulation of Investigatory Powers (Juveniles) Order 2000
- SI 2010 No.480 Regulation of Investigatory Powers (Communications Data) Order 2010
- SI 2010 No.521 Regulation of Investigatory Powers (Directed Surveillance and Covert Human Intelligence Sources) Order 2010
- SI 2010 No. 461 Regulation of Investigatory Powers (Extension of Authorisation Provisions: Legal Consultations) Order 2010
- SI 2012 No. 1500 Regulation of Investigatory Powers (Directed Surveillance and Covert Human Intelligence Sources) (Amendment) Order 2012

i) The Investigatory Powers Commissioner's Office:
PO Box 29105
London
SW1V 1ZU

email: info@ipco.org.uk

6.2 Complaints can be made to:

Maldon District Council, RIPA Senior Responsible Officer

(Who will ensure that they are passed to the relevant Authorising Officer for an initial response.)

Maldon District Council
Princes Road
Maldon
Essex
CM9 5DL
Tel: 01621 854477

The Investigatory Powers Tribunal:
PO Box 3322
London, SW1H 9ZQ
Tel: 0207 035 3711 www.ipt-uk.com

APPENDIX A

RIPA ADMINISTRATION:

Senior Responsible Officer
Richard Holmes

Director of Service Delivery and Head of Paid Service

Tel: 01621 854477 or 732767

Email: richard.holmes@maldon.gov.uk

RIPA Co-ordinating Officer
Spencer Clarke: Community Safety Manager (and Deputy Safeguarding Lead)
Tel: 01245 606477

Email: spencer.clarke@maldon.gov.uk

AUTHORISING OFFICERS:

Damien Ghela
Lead Specialist Community (and safeguarding Lead Officer)
Tel: 01621 854447
Email: damien.ghela@maldon.gov.uk

Annette Cardy
Resources Specialist Service Manager
Tel 2727
Email: annett.cardy@maldon.gov.uk

DESIGNATED OFFICERS:

Emma Holmes
Senior Legal Specialist and Data Protection Officer
Tel: 01621 732732
Email: emma.holmes@maldon.gov.uk

Grant Hulley
Senior ICT Specialist and Senior Information Responsible Officer
Tel: 07783 999804
Email: grant.hulley@maldon.gov.uk