REGULATION OF INVESTIGATORY POWERS ACT 2000 (RIPA)

1 PURPOSE OF REPORT

1.1 The purpose of this report is to update Members on the use of the RIPA over the past year and to allow for the review of the Council's RIPA policy.

2 INTRODUCTION

2.1 On 8 March 2011 Members of the Review Committee agreed to provide a strategic overview of the Council's use of RIPA powers in terms of reviewing the policy and considering regular statistical reports on usage.

2.2 On 12 July 2011 the Committee agreed that it would consider statistics and review the Council's RIPA policy annually.

3 ANNUAL STATISTICS ON THE COUNCIL'S USE OF RIPA POWERS

17 September 2021 – 17 September 2022

Authorisation Date	Nature of Authorisation	Expiry date / Review Date(s)/ Cancellation Date
NIL		

3.1 Members will note that the Council has not exercised its use of RIPA since 8 February 2011.

4 ANNUAL POLICY REVIEW

4.1 The Council last reviewed its RIPA Policy and RIPA Social Media Policy in October 2021. A specialist RIPA training company undertook the review and as a result a revised RIPA Policy and RIPA Social Media Policy was approved by Members at a meeting of the Review Committee on 26 November 2021.

4.2 The RIPA Policy has been reviewed and there are no amendments to consider other than a change of officers which have been reflected and amended accordingly.

5 RISK IMPLICATIONS

5.1 The improper or disproportionate use of RIPA powers could lead to adverse publicity in the media and serious reputational damage.

6 CRIME AND DISORDER IMPLICATIONS

6.1 The use of RIPA powers when necessary and proportionate may assist in the prevention and detection of crime.

7 RESOURCE IMPLICATIONS

7.1 There are no direct resource implications arising from this report.

8 LEGAL IMPLICATIONS

8.1 Failure to comply with RIPA legislation may mean that covert investigatory evidence will not be accepted in court and there may be issues of privacy/human rights contraventions, as well as a claim for damages.

9 EQUALITY AND DIVERSITY IMPLICATIONS

An Equality Impact Assessment has been completed and found there to be no impacts (either positive or negative) on protected groups as defined under the Equality Act 2010.

10 RECOMMENDATION

10.1 It is proposed that the Committee **RESOLVES**

That the Council's annual usage of RIPA be noted.

Tracey Lilley

Director of Communities & Health,

Background Papers:-

None.

For further information please contact Tracey Lilley on:-

Phone: 01277 312644
Email: Tracey.lilley@brentwood.rochford.gov.uk

If you would like this report in large print, Braille or another language please contact 01702 318111.

ROCHFORD DISTRICT COUNCIL

COVERT SURVEILLANCE POLICY AND PROCEDURE MANUAL

PURSUANT TO THE

REGULATION OF INVESTIGATORY POWERS ACT 2000

This manual has been prepared to assist officers who undertake covert surveillance but is not intended to be an exhaustive guide

Revised November 2022

GUIDANCE

1 PURPOSE

1.1 The Council's officers in the course of investigating regulatory criminal offences and in the interests of the safety and wellbeing of the district may be required to undertake covert monitoring operations to gather evidence to present to a court. In doing so those officers must comply with the relevant legislation i.e. the Regulation of Investigatory Powers Act 2000 (RIPA) and the associated regulations and codes of practice. Evidence collected without complying with the statutory procedures may become inadmissible and prejudice the outcome of the investigation and may be the subject to a complaint to the Investigatory Powers Tribunal (IPT) or a of a claim for damages under the Human Rights Act 1998.

2 SCOPE

2.1 This guidance applies to the planned deployment of directed covert surveillance or the use of Covert Human Intelligence Sources (CHIS) against specified individuals. The following provisions relate therefore to the observation of specified individuals from a vehicle, foot surveillance, the setting up of covert observation positions, the use of equipment for the monitoring of specified individuals and the use of informants or undercover operatives.

2.2 The Council's policy does not contemplate the monitoring of telephone use or portal use (communications data) other than in exceptional circumstances as this is unnecessary and disproportionate in most if not all local authority criminal investigations. Guidance regarding the acquisition of communications data is beyond the scope of this document and separate advice from the RIPA Senior Responsible Officer, Monitoring Officer should be obtained.

2.3 With the increasing use of social media there is a significant amount of information on an individual's social networking pages. This information might be relevant to an investigation being undertaken by the Council. Unguided research into the sites of suspects could fall within the remit of RIPA and therefore require authorisation prior to it being undertaken.

2.4 Information posted on Social Networking Sites may still be considered as private information and an authority may be required. This is because it is likely the intention of the individual when making such information available was not for it to be used for a covert purpose such as investigative activity by council officers. This is regardless of whether a user of a website or social media platform has sought to protect such information by restricting its access by activating privacy settings.

2.5 Repeated or persistent viewing of 'open source' sites, however, may also constitute directed surveillance but should be seen on a case-by-case basis e.g., if someone is being monitored through, for example, their Facebook profile for a period of time and a record of the information is kept for later analysis, this is likely to require a RIPA authorisation for directed surveillance. If, however, an officer merely wants to check on the accuracy of data known from elsewhere to ensure the investigation is directed at the correct person, then it will probably not attract the need for an authority.

2.6 To avoid the potential for inadvertent or inappropriate use of social network sites in investigative and enforcement roles, Officers should be mindful of any relevant guidance and refer to the Council's separate 'Use of Social Media in Investigations Policy and Procedure'.

3 BACKGROUND

3.1 Part II of the Regulation of Investigatory Powers Act 2000 (RIPA) provides a mechanism for public authorities to undertake certain investigative techniques in compliance with the Human Rights Act 1998. In particular it allows lawful interference with Article 8 of the European Convention of Human Rights, (the right to respect for private and family life).

3.2 The Home Office has issued revised Codes of Practice to provide guidance to public authorities on the use of RIPA to authorise covert surveillance that is likely to result in the obtaining of private information. The revised Codes of Practice are titled "Covert Surveillance and Property Interference" and "Covert Human Intelligence Sources".

3.3 All Codes of Practice issued pursuant to section 71 of RIPA are admissible as evidence in criminal and civil proceedings. If any provision of the Codes appears to be relevant to a court or tribunal considering any such proceedings, or to the Investigatory Powers Tribunal established under RIPA, or to one of the Commissioners responsible for overseeing the powers conferred by RIPA, they must be taken into account.

3.4 This Procedure sets out the procedures that must be followed when the Council undertakes authorised covert surveillance and brings into effect a number of changes that have been implemented by the revised Codes as well as recent changes to the law in this area. It is intended to be a good practice guide. This Manual is not intended to replace the Home Office Codes.

3.5 Those officers that intend to apply for an authorisation under RIPA must familiarise themselves with the appropriate Code of Practice as well as this Procedure. The Codes of Practice are available online https://www.gov.uk/government/collections/ripa-codes#current-codes-of-practice

3.6 The covert activity regulated by RIPA and covered by the above Codes of Practice is in three categories; intrusive surveillance, directed surveillance and covert human intelligence. The Act and Codes set up procedures for the authorisation of these activities.

3.7 The authorising officer should believe that the authorisation is necessary for the purpose of investigating crimes as directed surveillance can only be granted for the prevention and detection of crime which attract a maximum custodial sentence **of six months** or more or criminal offences relating to the underage sale of alcohol or tobacco and is a proportionate tactic. (See 7.3. 10.1)

3.8 Authorising officers and applicants (See Annex 1 and 2 for lists of named officers) should have regard to the Code of Practice 'Covert Surveillance and Property Interference' which states that obtaining an authorisation will only ensure that there is a justifiable interference with an individual's Article 8 Rights if it is necessary and proportionate for these activities to take place.

3.9 Authorising officers should first believe that the authorisation is necessary for the prevention and detection of crime or preventing disorder, namely an offence which carries a maximum custodial sentence **of six months** or more or criminal offences relating to the underage sale of alcohol or tobacco. Authorising officers should ask themselves if the evidence could be obtained in any other way? Is the surveillance operation required to obtain what the requesting officer is seeking to achieve? If there is a less intrusive means of obtaining the information, then the authorisation should not be granted. It needs to be remembered that whilst the authorising officer gives an authorisation, judicial approval of the authorisation will also be required before the surveillance takes place which is set out further at paragraph 9.

3.10 If the activities are considered necessary, the authorising officer must believe that the activity is proportionate to what is sought to be achieved by carrying it out and should consider the four elements of proportionality:

i. balancing the size and scope of the proposed activity against the gravity and extent of the perceived crime or harm.

ii. explaining how and why the methods to be adopted will cause the least possible intrusion on the subject 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 information sought;

iv. evidencing, as far as reasonably practicable, what other methods had been considered and why.

4 COVERT SURVEILLANCE

4.1 Covert surveillance means surveillance, which is carried out in a manner calculated to ensure that the persons subject to the surveillance are unaware that it is or may be taking place. There are two categories of covert surveillance defined in RIPA: intrusive surveillance and directed surveillance.

Intrusive Surveillance

4.2 Covert surveillance is "intrusive surveillance" if it:

- Is covert.
- Relates to residential premises and private vehicles; and
- Involves the presence of a person on the premises or **in** the vehicle or is carried out by a surveillance device on the premises or in the vehicle.
- Surveillance equipment mounted outside the premises will not be intrusive, unless the device consistently provides information of the same quality and detail as might be expected if they were in the premises or vehicle. This is unlikely in the case of equipment, such as a noise recorder when used to assess noise nuisance and volume levels, but care must be taken in setting up of equipment and locating the microphone.

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

Directed Surveillance

4.4 Directed surveillance, as defined in RIPA Section 26, is surveillance which is covert, but not intrusive and undertaken:

(a) For the purpose of a specific investigation or operation; and

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

(c) Otherwise than 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 this part to be sought for the carrying out of the surveillance.

5 COVERT HUMAN INTELLIGENCE SOURCES ("CHIS")

5.1 The Council is also permitted to use Covert Human Intelligence Sources under the Act. Under the 2000 Act. A person is a CHIS if:

a) they establish or maintain a personal or other relationship with a person for the covert purpose of facilitating the doing of anything falling within paragraph 26(8)(b) or (c);

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

c) they covertly disclose information obtained by the use of such a relationship or as a consequence of the existence of such a relationship.

A relationship is established or maintained for a covert purpose if and only if it is conducted in a manner that is calculated to ensure that one of the parties to the relationship is unaware of the purpose

5.2 At the current time the Council does not consider this necessary and **will not use** Covert Human Intelligence Sources.

5.3 It is the Policy of this authority that Council Officers **must not** use Covert Human Intelligence Sources.

5.4 Unlike directed surveillance, which relates specifically to private information, authorisations for the use or conduct of a Covert Human Intelligence Source do not relate specifically to private information, but to the covert use of a relationship to gain any information. European Court of Human Rights case law makes it clear that Article 8 of the European Convention on Human Rights includes the right to establish and develop relationships. Accordingly, any covert use of a relationship by a public authority (e.g., one party having a covert purpose on behalf of a public authority) is likely to engage Article 8, regardless of whether or not the public authority intends to acquire private information.

5.5 Not all human source activity will meet the definition of a Covert Human Intelligence Source. For example, a source may be a public volunteer who out of a sense of civic duty provide information that they have observed, or which is within their personal knowledge.

5.6 Certain individuals will be required to provide information to public authorities or designated bodies out of professional or statutory duty. For example, financial officials, accountants or company administrators may have a duty to provide information, to the Serious Fraud Office, that they have obtained by virtue of their position.

5.7 Any such regulatory or professional disclosures should not result in these individuals meeting the definition of a Covert Human Intelligence Source, as the business or professional relationships from which the information derives will not have been established or maintained for the covert purpose of disclosing such information.

5.8 Individuals or members of organisations (e.g., housing associations and taxi companies) who, because of their work or role have access to personal information, may voluntarily provide information to the public authorities on a repeated basis and need to be managed appropriately. Public authorities must keep such human sources under constant review to ensure that they are managed with an appropriate level of sensitivity and confidentiality, and to establish whether, at any given stage, they could meet the statutory definition of a Covert Human Intelligence Source.

5.9 Any officer concerned that a person meets this statutory definition must seek urgent advice from the Senior Responsible Officer.

6 AUTHORISATIONS

6.1 An authorisation for directed surveillance may only be authorised by the council on the following ground:

1) For the purpose of investigating criminal offences which attract a maximum custodial sentence **of six months** or more or criminal offences relating to the underage sale of alcohol or tobacco (see paragraph 10.1)

The authorising officer must believe that:

(a) The action is necessary on the ground set out in (1); and

(b) The surveillance is proportionate to what it seeks to achieve.

The Authorising Officer will be responsible for considering all applications for covert surveillance and for granting or refusing authorisations as appropriate. The Authorising Officer will also be responsible for carrying out reviews and ensuring that authorisations are renewed or cancelled where necessary.

6.2 The minimum position of an Authorising Officer has been designated by the Regulation of Investigatory Powers (Directed Surveillance and Covert Human Intelligence Sources) Order 2010. For a local authority the Authorising Officer must be the Director, Head of Service, Service Manager or equivalent.

6.3 The Council should also have in place a back-up system for situations where the Authorising Officer is unavailable to grant an authorisation and the situation becomes urgent. This will enable officers to identify the person who is able to give authorisations in the Authorising Officer's absence. It should be

noted that as a result of the Protection of Freedoms Act 2015, local authorities are not permitted to grant urgent authorisations, as all authorisations require judicial approval.

6.4 Wherever knowledge of confidential information, is likely to be acquired through the directed surveillance, a higher level of authorisation is needed. In the Council, this would be the Head of Paid Service (the Chief Executive) or the person acting as Head of Paid Service in their absence. Confidential Information is defined as:

- Legally privileged material.
- Communications between a Member of Parliament and another person on constituency matters.
- Confidential Personal Information (Confidential personal information is information held in confidence concerning an individual (whether living or dead) who can be identified from it, and the material in question relates to his or her physical or mental health or to spiritual counselling. Such information can include both oral and written communications).
- Confidential Journalistic Material.

6.5 A list of those officers who have been nominated as Authorising Officers is detailed Annex 1.

6.6 It is recommended best practice that there should be a Senior Responsible Officer (SRO) in each public authority who is responsible for:

- The integrity of the processes in place to authorise directed surveillance
- Compliance with RIPA and with the Codes of Practice
- Engagement with the Commissioners and inspectors when they conduct their inspections, and
- Where necessary, overseeing the implementation of any post-inspection action plans recommended or approved by a Commissioner.

6.7 As the SRO for a local authority is required be a member of the corporate leadership team, the Senior Responsible Officer for this Council will be the person named in Annex 1(b). The SRO will also be responsible for ensuring that all authorising officers are of an appropriate standard in light of the recommendations or concerns raised in the inspection reports prepared by the Investigatory Powers Commissioner's Office (IPCO) following their routine inspections.

6.8 The SRO will also undertake an annual audit of records and will be responsible for the day-to day quality control.

6.9 There is requirement for elected members of the Council to review the use of RIPA and to set the policy on covert surveillance at least once a year. The Council's Review Committee will review this Policy annually and ensure that it

is being used consistently with the Council's Policy. The Committee will report to Full Council, should they be of the opinion that it is not fit for purpose or requires amendment.

6.10 The Committee should not, and will not, be involved in making decisions on specific authorisations.

6.11 The RIPA Monitoring Officer (RMO) will be the person named in Annex 1(c). The role of the RMO is as follows:

- Maintaining the Central Record of authorisations and collating the original applications/authorisations, reviews, renewals and cancellations.
- Oversight of submitted RIPA documentation.
- Organising and maintain a RIPA training programme.
- Raising RIPA awareness within the Council.
- Appointment of investigating officers as authorised applicants by their inclusion in Annex 2.

AUTHORISATION PROCEDURE

7 STAGE 1 - Internal Authorisation

7.1 Any of the Council's authorised applicants (Annex 2) (who will invariably also be the investigating officer) may make an application for authorisation under RIPA to conduct a covert operation to an authorised officer (Annex 1). Any application for permission to conduct a covert operation must be in writing on the appropriate form. https://www.gov.uk/government/collections/ripa-forms--2

7.2 The standard forms used by all public authorities are listed in Schedule 1 of RIPA. The forms are an indication of the information required before an authorisation can be granted and are consistent with the requirements in the Codes of Practice. The Home Office recommends that all users of the form should add any information that is relevant to their organisation but avoid taking any information out of the forms.

7.3 A written application for authorisation must record:

(a) The action to be authorised, including any premises or vehicles involved
(b) The identities, where known, of those to be the subject of surveillance.
(c) A full account of the investigation or operation.
(d) Justifying that the authorisation is sought for investigating a crime which carries a maximum custodial sentence of 6 months or more or criminal offences relating to the underage sale of alcohol or tobacco is for the (see paragraph 10.1).
(e) How and why the investigation is both necessary and proportionate.

(f) Authorising Officer should state in their own words why the investigation is necessary and proportionate.

7.4 It is considered good practice for a simple sketch map of the immediate area of investigation, detailing specific observation points, location of monitoring equipment etc, to be appended to the application for authorisation.

8 CONSIDERATION

8.1 The investigating officer will keep notes during the initial stages of gathering intelligence. However, it should be stressed that the key document on which the authorising officer will base their decision is the application. Any formal notes made by the AO will be placed on the application form itself. Any rough notes made from meetings or briefings will be held on the case file.

8.2 Requests to the authorising officer for authorisation to mount a covert operation will be subject to and based on, the intelligence gathered and recorded on the investigator's notes which must be articulated in the application.

8.3 The officer will consider if such an operation would assist in investigating crimes which carry a maximum custodial sentence **of six months** or more or criminal offences relating to the underage sale of alcohol or tobacco. (see paragraph 10.1)

8.4 Responsibility for authorisation for a covert operation will be considered on the grounds that any operation is likely to be of value in connection with;

- investigating crimes which carry a maximum custodial sentence **of six months** or more or criminal offences relating to the underage sale of alcohol or tobacco. (See paragraph 10.1)

- and that the proposed covert operation is a reasonable means of achieving the desired result. This must be balanced with the individual's rights under the Human Rights Act 1998.

8.5 Any authorisation must be on the basis that the activity is both necessary and proportionate. The Authorising Officer must also take into account the risk of intrusion into the privacy of persons other than those directly implicated in the operation or investigation (collateral intrusion)

8.6 If there is any doubt, all Council officers should ask the SRO or RMO Officer **before** any directed surveillance is authorised, rejected, renewed or cancelled.

9 SERIOUS CRIME THRESHOLD

9.1 No officer may make an authorisation under this policy unless it concerns conduct which constitutes one or more criminal offences (or would do if it all took place in England and Wales) and either the criminal offence (or one of the criminal offences):

- Is or would be an offence which is punishable by a maximum term of at least 6 months of imprisonment; or
- Is an offence under:
  - i. Section 146 of the Licencing Act 2003(3) (sale of alcohol to children);
  - ii. Section 147 of the Licencing Act 2003 (allowing the sale of alcohol to children);
  - iii. Section 147A of the Licencing Act 2003(4) (persistently selling alcohol to children);
  - iv. Section 7 of the Children and Young Persons Act 1933(5) (sale of tobacco, etc., to persons under eighteen).

9.2 In exceptional circumstances, where no named authorising officer is available, any Service Manager or more senior appointment is prescribed within legislation as an authorising officer. They would not however be permitted to authorise unless they have previously received relevant RIPA training.

9.3 Officers should not authorise their own activities except as a matter of urgency.

10 DURATION AND REVIEW OF AUTHORISATIONS

10.1 Authorisations for directed surveillance will cease to have effect three months from the day of issue and for the use of covert human intelligence sources, twelve months. The expiry date and time on the directed surveillance authorisation form will therefore always be three months from the date of authorisation, controlled by review and cancellation. The effective time and date is the time the authority is approved by the Magistrate, not the time of signing by the AO. Authorisations should be reviewed on a regular basis, using the appropriate form, to ensure that they are still necessary and proportionate.

10.2 Authorisations can be renewed prior to their expiry providing the criteria in paragraph 3.9 and the Code of Practice is met. Applications for renewal must be in writing and the application and the decision, detailing the grounds for the renewal or refusal to renew or withdrawal of the authorisation. All renewals must receive judicial approval from a magistrate prior to taking effect.

10.3 When the need for the authorisation has ceased i.e., at any point when the authorisation for covert surveillance is no longer required or no longer meets the criteria for authorisation, the authorisation must be cancelled by the

authorising officer using the appropriate form. At the end of the authorisation period, if not cancelled previously, it must be cancelled not simply allowed to expire.

10.4 Any authorisation needs to be formally reviewed to ensure the use of tactic is still required, the activity authorised remains the activity deployed.

10.5 A review must take place one month and every month after the authorisation at minimum, but it is accepted as good practice that the authority is reviewed at milestones throughout the use of the tactic. The frequency is determined by the AO and can be at any time if required depending on circumstances. A review is a formal process and is completed on the relevant review form.

10.6 Particular attention should be given to the need to review authorisations frequently where they involve a high level of intrusion into private life, significant collateral intrusion, or confidential information is likely to be obtained.

11 STAGE 2 - JUDICIAL OVERSIGHT AND APPROVAL

11.1 The *Protection of Freedoms Act* brought into law the Judicial oversight of all RIPA approvals by Local Authorities. It inserts sections into the 2000 Act which mean that authorisations whilst still given by council officers, do not take effect until a Magistrate has approved them. The Judicial oversight does not take the place of the current authorisation process – it is an oversight function and not an authorisation function. The Authority may not undertake the regulated activity until *Judicial Approval* has been given.

11.2 The Authority has appointed authorised applicants, to make applications under this part (Annex 2) (in accordance with s.223(1) of the Local Government Act 1972), subject to their inclusion in the approved list at annex 2 by the *RMO.* The Authority has authorised the *RMO* to appoint as many investigation officers and managers to make applications under this part as they sees fit. Those officers must be listed at annex 2 and any decisions to or deletions from that list must be notified to Members as part of the regular reporting protocols.

11.3 Once the application has been approved by an officer listed in Annex 1, the Authority must apply to the Magistrates Court for an order confirming that:

a. The person who granted or renewed the authorisation was entitled to do so;
b. The grant or renewal met the relevant restrictions or conditions;
c. There were reasonable grounds for believing (at the time it was made or renewed) that obtaining the information described in the form was both necessary and proportionate; and

d. It is still (at the time the court considers it) reasonable to believe the grant/renewal to be both necessary and proportionate.

11.4 The oversight will be determined at a hearing in front of a single Magistrate or District Judge. An officer appointed to do so (and listed at Annex 2 i.e. also the authorised applicant) must approach the court office to arrange the hearing.

11.5 The authorised applicant must submit a form, along with electronic copies of any accompanying documents (set out below) to the *Authorising Officer* for consideration. Once satisfied with the standard of the form and any attachments, the *Authorising Officer* must submit the bundle electronically to the *RMO* for onward transmission to the courts.

11.6 The bundle for submission to the courts must include:

a. The application for the order approving the authorisation;
b. The authorised application or renewal form;
c. Any supporting information, that exceptionally, does not form part of the form;
d. Any information you have that might show a reason to refuse the application;
e. An extract from the relevant legislation showing the offence being investigated and that it carries the relevant maximum sentence (unless it is one of the offences provided for in 7A(3)(b) of the 2010 regulations and
f. A copy of the Annexes 1 and 2 to this policy, showing that the *Authorising Officer* and the *Authorised Applicant* are both persons duly approved to carry out those functions by the Authority.

11.7 The form requires that the authorised applicant makes a declaration of truth and disclosure, as part of the application for Judicial approval. **It is important that this is not signed lightly;** check that all material facts have been disclosed within the bundle and that the contents are accurate and true.

11.8 The authorised applicant must attend the hearing and assert the accuracy of the application.

11.9 The applicant must also be prepared to answer any questions about the application and the investigation which the Magistrate may have. At the end of the application, the magistrate will give the Court's decision.

11.10 Once the bundle has been submitted the *RMO* will note this in the central record. Within 24 hours of receiving the Court's decision, the applicant must

notify the *RMO* and the *Authorising Officer* by sending them an email. Both parties must also be sent copies of any court order. The original must be retained on the investigation file. The *RMO* will note the record of the outcome.

11.11 In the event that the Court refuses the application, the authorised applicant, the *Authorising Officer* and the *RMO* will review the decision within 24 hours and decide if they wish to make representations to the Court before a *Quashing Order* is made.

11.12 If the Authority decides to make representations about a refused application, the *Authorising Officer and RMO* will immediately notify the court officer of this and request a hearing.

11.13 Grounds for the submission should be set out in writing and notified to the court before the hearing. It must be drafted by the applicant and approved by the *Authorising Officer and RMO.* It must contain the standard declaration as set out above.

11.14 If the Authority elects to seek a hearing, the applicant, *Authorising Officer* and *RMO* will attend the hearing.

11.15 At the conclusion of the hearing, the *RMO* will note the outcome in the central record.

12 CENTRAL RECORD OF ALL AUTHORISATIONS

12.1 The RIPA Monitoring Officer will maintain a central record of all authorisations granted, renewed or cancelled by the council. These records to be made available to the relevant Commissioner or an Inspector from the Investigatory Powers Commissioner's Office, upon request.

12.2 Within one week of the relevant date, a copy of the application, review, renewal, court order and cancellation form are to be placed and kept secure in the RIPA Records File by the Corporate Services team.

12.3 All records shall be retained for a minimum of three years to ensure that they are available for inspection by the Commissioner.

12.4 Where there is a belief that the material relating to an investigation could be relevant to pending or future criminal or civil proceedings, it should be retained in accordance with the Criminal Procedure and Investigations Act 1996 and kept a period of at least five years.

13 SAFEGUARDS (PRIVILEGED and CONFIDENTIAL INFORMATION)

13.1 Public authorities should ensure that their actions when handling information obtained by means of covert surveillance comply with relevant legal frameworks and this code, so that any interference with privacy is justified in accordance with Article 8(2) of the European Convention on Human Rights. Compliance with these legal frameworks, including data protection requirements, will ensure that the handling of private information so obtained continues to be lawful, justified and strictly controlled, and is subject to robust and effective safeguards.

13.2 All material obtained under the authority of a covert surveillance authorisation must be handled in accordance with safeguards which the public authority has implemented in line with the requirements of this code. These safeguards should be made available to the Investigatory Powers Commissioner. Breaches of these safeguards must be reported to the Commissioner in a fashion agreed with him or her. Any breaches of data protection requirements should also be reported to the Information Commissioner. Public authorities must keep their internal safeguards under periodic review to ensure that they remain up to date and effective. During the course of such periodic reviews, public authorities must consider whether more of their internal arrangements might safely and usefully be put into the public domain and further engage with the Publication Scheme as described in the Freedom of Information Act 2012.

13.3 Dissemination, copying and retention of material must be limited to the minimum necessary for authorised purposes. For the purposes of this policy, something is necessary for the authorised purposes if the material:

- is, or is likely to become, necessary for a statutory purpose in relation to covert surveillance or property interference;
- is necessary for facilitating the carrying out of the functions of public authorities under RIPA, CPIA 1996, the Data Protection Act or Freedom of Information Act;
- is necessary for facilitating the carrying out of any functions of the Commissioner or the Investigatory Powers Tribunal;
- is necessary for the purposes of legal proceedings; or
- is necessary for the performance of the functions of any person by or under any enactment.

13.4 Material obtained through directed surveillance, may be used as evidence in criminal proceedings. The admissibility of evidence is governed primarily by the common law, the Criminal Procedure and Investigations Act 1996, the Civil Procedure Rules, section 78 of the Police and Criminal Evidence Act 1984 and the Human Rights Act 1998

13.5 Ensuring the continuity and integrity of evidence is critical to every

prosecution. Accordingly, considerations as to evidential integrity are an important part of the disclosure regime under the Criminal Procedure and Investigations Act 1996 and these considerations will apply to any material acquired through covert surveillance that is used in evidence. When information obtained under a covert surveillance authorisation is used evidentially, the public authority should be able to demonstrate how the evidence has been obtained, to the extent required by the relevant rules of evidence and disclosure.

13.6 Each public authority must ensure that there are internal arrangements in force in relation to dealing with any private information obtained by these means. Authorising officers, through their relevant Data Controller, must ensure compliance with the appropriate data protection requirements under the Data Protection Act 2018 and any relevant internal arrangements produced by individual authorities relating to the handling and storage of material.

13.7 The number of persons to whom any of the information is disclosed or copied, and the extent of disclosure / copying, should be limited to the minimum necessary for the authorised purpose(s) set out in 13.3 above. This obligation applies equally to disclosure / copying to additional persons within a public authority and to disclosure / copying outside the authority. In the same way, only so much of the material may be disclosed as the recipient needs; for example, if a summary of the material will suffice, no more than that should be disclosed.

13.8 Material obtained through covert surveillance and all copies, extracts and summaries of it, must be handled and stored securely, so as to minimise the risk of loss or theft. It must be held so as to be inaccessible to persons without the required level of security clearance (where applicable). This requirement to store such material securely applies to all those who are responsible for the handling of the material. In particular, the SRO must ensure the following protective security measures are applied:

- physical security to protect the information where it may be stored or accessed.
- IT security to minimise the risk of unauthorised access to IT systems.
- an appropriate security clearance regime for personnel which is designed to provide assurance that those who have access to this material are reliable and trustworthy

13.9 Information obtained through covert surveillance and all copies, extracts and summaries which contain such material, should be scheduled for deletion or destruction, and securely destroyed as soon as they are no longer needed for the authorised purpose(s) set out in 13.3 above. If such information is retained, it should be reviewed at appropriate intervals to confirm that the justification for its retention is still valid. In this context, destroying material means taking such steps as might be necessary to make access to the data

impossible.

13.10 Where the product of surveillance could be relevant to pending or future criminal or civil proceedings (see 13.3), it should be retained in accordance with established disclosure requirements. In the case of the Council, particular attention is drawn to the requirements of the code of practice issued under the Criminal Procedure and Investigations Act 1996, which requires that the investigator retain, record, reveal, review all material obtained in an investigation which may be relevant to the investigation.

13.11 In practice, it is unlikely surveillance authorised and carried out by the Council would involve confidential information. However, where there is a possibility that the use of surveillance will enable knowledge of confidential information to be acquired e.g., conversations between a doctor and patient, a higher level of authority for such surveillance is required.

13.12 Confidential personal information is information held in confidence concerning an individual (whether living or dead) who can be identified from it, and the material in question relates to his or her physical or mental health or to spiritual counselling, constituent correspondence, journalistic material held in confidence and legal privilege material. Such information can include both oral and written communications.

13.13 In cases where it is likely that knowledge of confidential information will be acquired, the use of covert surveillance is subject to a higher level of authorisation, namely by the Head of Paid Service (Chief Executive) or, in their absence, the Chief Officer acting as Head of Paid Service.

13.14 Any case where confidential information is obtained and retained, the matter should be reported to the Investigatory Powers Commissioner as soon as reasonably practicable, and any material which has been obtained and retained should be made available to the Commissioner on request so that the Commissioner can consider whether the correct procedures and considerations have been applied.

13.15 The authorised applicant should complete the application form for authorisation of directed surveillance in the usual way, but with sufficient indication of the likelihood that confidential information will be acquired.

13.16 At all times during any operation officers are to conduct themselves in a manner that will not breach

- The Human Rights Act 1998
- Regulation of Investigatory Powers Act 2000
- Data Protection Act 2018
- This Guidance & Working Code of Practice

- *Any relevant code of practice issued by the Home Office.*

14 COMPLAINTS

14.1 There is provision under RIPA for the establishment of an independent Tribunal. This Tribunal will be made up of senior members of the legal profession or judiciary and will be independent of the Government.

14.2 The Tribunal has full powers to investigate and decide upon complaints made to them within its jurisdiction, including complaints made by a person who is aggrieved by any conduct to which Part II of RIPA applies, where he believes such conduct to have taken place in "challengeable circumstances" or to have been carried out by or on behalf of any of the intelligence services.

14.3 Conduct takes place in "challengeable circumstances" if it takes place:

(i) with the authority or purported authority of an authorisation under Part II of the Act; or

(ii) the circumstances are such that it would not have been appropriate for the conduct to take place without authority; or at least without proper consideration having been given to whether such authority should be sought.

14.4 Further information on the exercise of the Tribunal's functions and details of the relevant complaint's procedure can be found here https://www.ipt-uk.com/

14.5 Notwithstanding the above, members of the public will still be able to avail themselves of the Council's internal complaints procedure, where appropriate, which ultimately comes to the attention of the Local Government Ombudsman.

15 THE INVESTIGATORY POWERS COMMISSIONERS' OFFICE

15.1 The Act also provides for the independent oversight and review of the use of the powers contained within Part II of RIPA, by a duly appointed Investigatory Powers Commissioner.

15.2 The Investigatory Powers Commissioners Office (IPCO) was established to oversee covert activity carried out by public authorities and within this office a team of Judicial Commissioners and Inspectors has been formed, to assist the Investigatory Powers Commissioner in the discharge of their review responsibilities.

15.3 One of the duties of the IPCO is to carry out planned inspections of those public authorities who are authorised carry out surveillance and the use of Covert Human Intelligence Sources as specified in RIPA, to ensure compliance with the statutory authorisation procedures. At these inspections,

policies and procedures in relation to directed surveillance and CHIS operations will be examined and there will be some random sampling of selected operations. The central record of authorisations will also be inspected. Chief Officers will be given at least two weeks' notice of any such planned inspection.

15.4 An inspection report will be presented to the Chief Officer, which should highlight any significant issues, draw conclusions and make appropriate recommendations. The aim of inspections is to be helpful rather than to measure or assess operational performance.

15.5 In addition to routine inspections, spot checks may be carried out from time to time.

15.6 There is a duty on every person who uses the powers provided by Part II of RIPA, which governs the use of covert surveillance or covert human intelligence sources, to disclose or provide to the Investigatory Powers Commissioner, supported by Judicial Commissioners (or his duly appointed Inspectors) all such documents and information that he may require for the purposes of enabling him to carry out his functions.

IMPORTANT NOTE

This Procedure Manual has been produced as a guide only and is primarily based on the revised Codes of Practice on Covert Surveillance and Covert Human Intelligence Sources published by the Home Office. These Codes can be found https://www.gov.uk/government/collections/ripa-codes

For further information please contact:

Tracey Lilley – Director for Communities & Health
RIPA Senior Responsible Officer
tracey.lilley@brentwood.rochford.gov.uk

ANNEX 1

Appointment of Authorised Officers

The following officers have been appointed by the Council as Authorising Officers for the purposes of RIPA:

- Steve Summers (Strategic Director)
- Marcus Hotten (Director Environment)
- Andrew Paddon (Environmental Health Team Leader)

Senior Responsible Officer

- Tracey Lilley, Director Communities & Health

RIPA Monitoring Officer

- Angela Law, Assistant Director, Legal & Democratic Services

ANNEX 2

Council's Authorised Applicants

In order for the Authority's RIPA authorisations to take effect, they must be approved by a Magistrate. That process requires applicants in person to appear for the Authority.

Any person from this Authority wishing to make an application must be named in this annex and must take to court a copy of this annex and their official identification. The following have been appointed under section 223(1) of the Local Government Act 1972 to appear for the Authority and are approved applicants in accordance with paragraph 9.2 of this policy:

Name	Section	Appointed from
Caroline Bell	Street Scene	15/04/14
Jane Spink	Environmental Health	15/04/14
Yvonne Dunn	Planning	15/04/14
Andrew Paddon	Environmental Health	15/04/14
Steven Greener	Licensing	17/10/17
Adrian Hills	Street Scene	17/10/17
Talent Masuku	Planning Enforcement	17/10/17
Tara Miller	Environmental Health	17/10/17
Siobhan Sheridan	Environmental Health	17/10/17
Mark Stanbury	Environmental Health	11/12/18
Andy Parkman	Community Safety Officer	08/10/19
Peter Miles	Revenues & Benefits Counter fraud and Compliance officer	08/11/21

Signed…….

Angela Law RIPA Monitoring Officer