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 RIPA over the past year and to allow for the review of the Council's RIPA policy. It also makes some recommendations to amend certain aspects of the policy that have arisen due to staff changes during the year.

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 quarterly and annual statistical reports on usage.

2.2 On 12 July 2011 the Committee agreed that in the interests of saving resources, it would consider statistics and review the Council's RIPA policy on an annual rather than quarterly basis.

2.3 The last report to this Committee regarding RIPA usage was on 6 November 2018, which also proposed changes to the Council's RIPA policy.

2.4 Officers received RIPA training on 16 March 2018 and on 13 July 2018 with further training being proposed for early 2020.

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

18 September 2018 – 17 September 2019

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

3.1 Members will note that the Council is a sparing user of RIPA powers, the last authorisation having been made on 8 February 2011.

4 ANNUAL POLICY REVIEW

4.1 The Council's RIPA policy was updated on 11 December 2018 and took account of the comments of the Investigatory Powers Commissioner's office resulting from their table-top inspection.

4.2 Some further minor amendments are required to be made to the policy, as follows:

Page 6.21 Delete Martin Howlett (Environmental Health Team Leader) from the list of Authorising Officers.

Page 6.22 Delete Martin Howlett (Environmental Health Team Leader) from the list of Authorised applicants.

Page 6.22 Add Andy Parkman (Community Safety Officer) to the list of Authorised applicants.

An amended version of the policy is attached as an appendix to this report

5 RISK IMPLICATIONS

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

7 CRIME AND DISORDER IMPLICATIONS

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

9 RESOURCE IMPLICATIONS

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

10 LEGAL IMPLICATIONS

10.1 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.

11 EQUALITY AND DIVERSITY IMPLICATIONS

12 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.

13 RECOMMENDATION

13.1 It is proposed that the Committee **RESOLVES** to note the Council's annual usage of RIPA.

13.2 It is proposed that the Committee **RECOMMENDS** to Council that the amendments to the Council's RIPA policy set out in section 4 above are approved.

Louisa Moss

Assistant Director People & Communities

Background Papers:-

None.

For further information please contact Louisa Moss on:-

Phone: 01702 318095
Email: Louisa.Moss@rochford.gov.uk

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

APPENDIX

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

Louisa Moss

Assistant Director People & ~~CommuntiesCommunitiesCommunity & Housing Services~~
RIPA Senior Responsible Officer

GUIDANCE

1 PURPOSE

1.1 The Council's officers in the course of investigating frauds, regulatory criminal offences and in the interests of the safety and well being 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 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 in such a manner as is likely to result in obtaining private information about the person. 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 officers.

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. However, 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 Where privacy settings are available but not applied the data available on Social Networking Sites may be considered 'open source' and an authorisation is not usually required.

2.5 Repeat viewing of 'open source' sites, however, may constitute directed surveillance on a case by case basis and this should be borne in mind 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.

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 the Council's separate 'Use of Social Media in Investigations Policy and Procedure' attached at Annex 1 of this Policy.

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 6 (right to a fair trial) and Article 8 (right to respect for private and family life) rights.

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 appear 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 best 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 and in the G/Shared/RIPA/Code of Practice area.

3.6 The covert surveillance 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 first satisfy themselves that the authorisation is necessary for the purpose of investigating crimes which carry a custodial sentence of 6 months or more (see paragraph

10.1 below) and that the surveillance is proportionate to what it seeks to achieve. Authorising and requesting officers (See Annex 1 and 2 for lists of named officers) should have regard to the Code of Practice "Covert Surveillance and Property Interference" , paragraphs 3.3 - 3.6. This 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.

3.8 It first requires authorising officers to believe that the authorisation is necessary in the circumstances of the particular case which further to changes to the law, means for the purpose of investigating crimes which carry a custodial sentence of 6 months or more (see paragraph 10.1) Authorising officers should ask themselves if the evidence could be obtained in any other way? Is the surveillance operation really necessary to what the requesting officer is seeking to achieve? Should there be a less intrusive means of obtaining the information, then the authorisation should not be granted. Judicial approval of the authorisation will also be required before the surveillance takes place which is set out further at paragraph 9

3.9 If the activities are considered necessary, the authorising officer must then satisfy himself that they are proportionate to what is sought to be achieved by carrying them out. He should consider the four elements of proportionality:

i) balancing the size and scope of the operation against the gravity and extent of the perceived mischief,
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 the only reasonable way, having considered all others, of obtaining the necessary result, and
iv) evidencing, as far as reasonably practicable, what other methods had been considered and why they were not implemented.

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 in the premises or **in** the vehicle or is carried out by a surveillance device in the premises or 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 DAT recorder when used to assess noise nuisance but care must be taken in setting up of equipment and locating the microphone.

4.3 This form of surveillance can therefore 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, as 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. A Covert Human Intelligence Source is someone who establishes or maintains a personal or other relationship for the covert purpose of helping the covert use of the relationship to obtain information. However at the current time the Council does not consider this necessary and will not use Covert Human Intelligence Sources.

5.2 All officers are strictly prohibited from using Covert Human Intelligence Sources.

5.3 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 manipulation 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 manipulation 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.

5.4 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 discloses information out of professional or statutory duty, or has been tasked to obtain information other than by way of a relationship.

5.5 Certain individuals will be required to provide information to public authorities or designated bodies out of professional or statutory duty. For example, employees within organisations regulated by the money laundering provisions of the Proceeds of Crime Act 2002 will be required to comply with the Money Laundering Regulations 2003 and report suspicious transactions. Similarly, financial officials, accountants or company administrators may have a duty to provide information that they have obtained by virtue of their position to the Serious Fraud Office.

5.6 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.

5.7 Individuals or members of organisations (e.g. travel agents, housing associations and taxi companies) who, because of their work or role have access to personal information, may voluntarily provide information to the police 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 be regarded as a Covert Human Intelligence Source.

5.8 Any officer concerned 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:

for the purpose of investigating crimes which carry a custodial sentence of 6 months or more or for offences relating to the sale of alcohol or tobacco to children and those under 18 (see paragraph 10.1)

The authorising officer must believe that:

(a) The action is necessary on the ground set out above; 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 office, rank or 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 a written 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.

6.4 Wherever knowledge of confidential information, such as a doctor's report, is likely to be acquired through the directed surveillance, a higher level of authorisation is needed. In the Council, this would be the Head or Paid Service (the Chief Executive) or the person acting as Head of Paid Service in his absence.

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

6.6 It is also now 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 has to be a member of the corporate leadership team, the Senior Responsible Officer for this Council will be the person named in Annex 1(b). She 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 Office of Surveillance Commissioners 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 also now a 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. Therefore, the Review Committee will review this Policy every 12 months and will report to Full Council, should they be of the opinion that it is not fit for purpose or requires amendment.

6.10 The Review Committee will also consider the Council's use of RIPA every 12 months to ensure that it is being used consistently with the Council's Policy.

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

6.12 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. The forms listed below are standard forms for use by all public authorities that 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.

7.2 Forms for the application, review, renewal or cancellation of authorisations are available in the Council's G/shared/RIPA/RIPA forms file.

Directed Surveillance

- DIRECT1 – Authorisation Directed Surveillance
- DIRECT2 – Review of a Directed Surveillance Authorisation
- DIRECT3 – Renewal of a Directed Surveillance Authorisation
- DIRECT4 – Cancellation of a Directed Surveillance Authorisation
- JUDICIAL1 – application for judicial approval for authorisation to conduct directed surveillance

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) Justifiying that the authorisation is sought for investigating a crime which carries a custodial sentence of 6 months or more (see paragraph 10.1)
(e) How and why the investigation is both necessary and proportionate.
(f) Authorising Officer should state in his 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. Further details on completing a written application for authorisation are contained in the Codes of Practice.

8 CONSIDERATION

8.1 The investigating officer will keep notes during the initial stages of gathering intelligence. Such records 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. The officer will consider if such an operation would assist in investigating crimes which carry a custodial sentence of 6 months or more (see paragraph 10.1)

8.3 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 custodial sentence of 6 months or more (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.

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

8.5 If in doubt, ask the SRO or RMO Officer BEFORE any directed surveillance is authorised, rejected, renewed or cancelled.

9 SERIOUSNESS 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 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 authorisation form will therefore always be three/twelve months from the date of authorisation, controlled by review and cancellation. 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 Conduct 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.

10.3 When the case is closed prior to the authorisation expiring or covert surveillance is no longer required or meets the criteria for authorisation, which ever is the sooner, the authorisation must be cancelled by the authorising officer using the appropriate form.

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 staff, 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 all investigation officers and managers 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 he 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, or the notice, 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 There is a form held in G/Shared/RIPA/RIPA forms/JUDICIAL1 that must accompany all applications. The authorised applicant (normally the *Officer in Charge* of the case) must complete this form electronically, once the *Authorising Officer* has approved the application. (This also applies to requests for renewals of authorisations.)

11.6 Once the form has been completed, the authorised applicant must submit this, along with electronic copies of any accompanying documents (set out below) to the *Authorising Officer for checking.* 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.

11.7 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 (see 10.1 below) 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.

11.8 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.

11.9 The authorised applicant must attend the hearing and assert the accuracy of the application. They 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 SRO, Assistant Director Community & Housing Services 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 Office of Surveillance Commissioners, upon request.

12.2 Within one week of the relevant date, a copy of the application, review, renewal, court order and cancellation form is to be placed in the RIPA Records File kept secure by the Leadership support 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. 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 CONFIDENTIAL INFORMATION

13.1 There are no special provisions under RIPA for the protection of "confidential information". Nevertheless, special care needs to be taken where the subject of the investigation or operation might reasonably expect a high degree of privacy or where confidential information is involved.

13.2 Confidential Information can include matters that are subject to legal privilege, confidential personal information or confidential journalistic material.

13.3 In practice, it is likely that most of the surveillance authorised and carried out by the Council would not 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.

13.4 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 his/her absence, the Chief Officer acting as Head of Paid Service.

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

13.6 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 1998
- The Council's Enforcement Concordat
- This Guidance & Working Code of Practice
- Any 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 complaints procedure can be obtained from:

Investigatory Powers Tribunal

PO Box 33220
London
SW1H 9ZQ

020 7273 4514

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 Chief Investigatory Powers Commissioner.

15.2 The Investigatory Powers Commissioners Office (IPCO) was established to oversee covert surveillance carried out by public authorities and within this Office an Inspectorate has been formed, to assist the Chief Investigatory Powers Commissioner in the discharge of his review responsibilities.

15.3 One of the duties of the IPCO is to carry out planned inspections of those public authorities who carry out surveillance 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 Chief Commissioner (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.

<u>IMPORTANT NOTE</u>

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 at www.homeoffice.gov.uk.

For further information please contact:

Louisa Moss – Assistant Director People & Communitiesy ~~& Housing Services,~~ RIPA Senior Responsible Officer– 01702 318095, EXT 3408 Louisa.moss@rochford.gov.uk
Angela Law – Assistant Director (Legal) Monitoring Officer, RIPA Monitoring Officer– 01702 318131, EXT 3701 angela.law@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:

~~Martin Howlett (Environmental Health Team Leader)~~

Paul Gowers (Overview & Scrutiny Officer)

Marcus Hotten (Assistant Director Place & Environment~~Environmental Services))~~

Shaun Scrutton (Managing Director and Head of Paid Service)

1(b) Senior Responsible Officer

Louisa Moss, Assistant Director People & Communities~~y & Housing Services~~

1(c) RIPA Monitoring Officer

Angela Law, Assistant Director (Legal) Monitoring Officer

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 and the official court service guidance makes it clear that these should be investigators not lawyers.

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.

I certify that 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	Appointment terminated
Caroline Bell	Street Scene	15/04/14	
Jane Spink	Environmental Health	15/04/14	
Lesley Athey	Street Scene	15/04/14	
Yvonne Dunn	Planning Enforcement	15/04/14	
~~Martin Howlett~~	~~Environmental Health~~	~~15/04/14~~	
Janette Fowler	Licensing	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	
Angela Brown	Environmental Health	17/10/17	
Mark Stanbury	Environmental Health	11/12/18	

Andy Parkman	Community Safety Officer		

Signed……..
Angela Law
RIPA Monitoring Officer

Use of Social Media in Investigations Policy and Procedure

A guide to the Council's approach to the use of social media in relation to Regulation of Investigatory Powers Act 2000 investigations.

USE OF SOCIAL MEDIA IN INVESTIGATIONS

POLICY AND PROCEDURES

CONTENTS

		Page
1.	Introduction & Background	3
2.	Regulation of Investigatory Powers Act 2000 (RIPA)	4
3.	What is Meant by 'Social Media' for the purposes of this Policy	4
4.	Privacy Settings	5
5.	What Is Permitted Under this Policy	6
6.	What Isn't Permitted Under this Policy	7
7.	Capturing Evidence	8
8.	Other IT Tools Available for Investigative Purposes	9
9.	Retention and Destruction of Information	9
10.	Policy Review	10

1 INTRODUCTION & BACKGROUND

1.1 Social Media has become a significant part of many people's lives. By its very nature, Social Media accumulates a sizable amount of information about a person's life, from daily routines to specific events. Their accessibility on mobile devices can also mean that a person's precise location at a given time may also be recorded whenever they interact with a form of Social Media on their devices. All of this means that incredibly detailed information can be obtained about a person and their activities.

1.2 Social Media can therefore be a very useful tool when investigating alleged offences with a view to bringing a prosecution in the courts. The use of information gathered from the various different forms of Social Media available can go some way to proving or disproving such things as whether a statement made by a defendant, or an allegation made by a complainant, is truthful or not. However, there is a danger that the use of Social Media can be abused, which would have an adverse effect, damaging potential prosecutions and even leave the Council open to complaints or criminal charges itself.

1.3 This Policy sets the framework on which the Council may utilise Social Media when conducting investigations into alleged offences. Whilst the use of Social Media to investigate is not automatically considered covert surveillance, its misuse when conducting investigations can mean that it crosses over into the realms of covert and/or targeted surveillance, even when that misuse is inadvertent. It is therefore crucial that the provisions of the Regulation of Investigatory Powers Act 2000 (RIPA), as it relates to covert and directed surveillance, are followed at all times when using Social Media information in investigations.

1.4 It is possible for the Council's use of Social Media in investigating potential offences to cross over into becoming unauthorised surveillance, and in so doing, breach a person's right to privacy under Article 8 of the Human Rights Act. Even if surveillance without due authorisation in a particular instance is not illegal, if authorisation is not obtained, the surveillance carried out will not have the protection that RIPA affords and may mean it is rendered inadmissible.

1.5 It is the aim of this Procedure to ensure that investigations involving the use of Social Media are done so lawfully and correctly so as not to interfere with an accused's human rights, nor to require authorisation under RIPA, whilst ensuring that evidence gathered from Social Media is captured and presented to court in the correct manner.

1.6 Officers who are involved in investigations, into both individuals and business they suspect to have committed an offence, should consult a RIPA Authorising Officer if they are unsure about any part of this Policy and how it affects their investigative practices.

2 REGULATION OF INVESTIGATORY POWERS ACT 2000 (RIPA)

2.1 With the increasing use of smartphones and personal devices, there is a significant amount of information on an individual's Social Media pages. This information might be relevant to an investigation being undertaken by the Council. However, unguided research into the sites of suspects could fall within the remit of RIPA and therefore require authorisation prior to it being undertaken. Officers should therefore seek advice from a RIPA Authorising Officer prior to undertaking any investigation using Social Media sites.

2.2 Officers embarking on any form of investigatory action should always do so with RIPA in mind. Whilst RIPA will not always be relevant to every investigation, it is vital that officers involved in investigative practices against individuals, regularly review their conduct with respect to investigatory actions. Any investigation is capable of evolving from being one that does not require RIPA authorisation, to one that does, at any point.

2.3 Accordingly, this Policy should be read in conjunction with the Council's current Covert Surveillance Policy and Procedure Manual, as well as the statutory codes of practice issued by the Secretary of State and the Investigatory powers Commissioner's office Guidance.

2.4 Instances of repeated and/or regular monitoring of Social Media accounts, as opposed to one-off viewing, may require RIPA authorisation. Advice should be sought from a RIPA Authorising Officer where it is envisaged that this level of monitoring will be required in relation to a particular investigation.

3 WHAT IS MEANT BY 'SOCIAL MEDIA' FOR THE PURPOSES OF THIS POLICY

3.1 Social Media, sometimes also referred to as a Social Network, can take many forms. This makes defining Social Media, for the purposes of this policy, difficult, however there are some facets which will be common to all forms of Social Media.

3.2 Social Media will always be a web-based service that allows individuals and/or businesses to construct a public or semi-public profile. Beyond this, Social Media can be very diverse, but will often have some, or all, of the following characteristics;

- The ability to show a list of other users with whom they share a connection; often termed "friends" or "followers",
- The ability to view and browse their list of connections and those made by others within the system

- Hosting capabilities allowing users to post audio, photographs and/or video content that is viewable by others

3.3 Social Media can include community based web sites, online discussions forums, chatrooms and other social spaces online as well.

3.4 Current examples of the most popular forms of Social Media, and therefore the most likely to be of use when conducting investigations into alleged offences, include:

Facebook	Twitter	Instagram
LinkedIn	Pintrest	Tumblr
Reddit	Flickr	Google+

3.5 The number and type of Social Media available to the public is fluid. In a given year, many new sites can open whilst some of the more established names can wain in popularity. This Policy will concentrate on Social Media generally and will not make reference to specific sites or services.

4 PRIVACY SETTINGS

4.1 The majority of Social Media services will allow its users to decide who can view their activity, and to what degree, through the use of privacy settings. Whilst some users are happy, or otherwise indifferent about who is able to view their information, others prefer to maintain a level of privacy.

4.2 Depending on their intentions, many users will purposely use Social Media with no privacy setting applied whatsoever. This could be due to the fact that they are actively promoting something, such as a business or event, and therefore require as many people as possible to be able to view their Social Media profile at all times; others may do so for reasons of self promotion or even vanity. The information publicly available is known as an individual's public profile.

4.3 Those individuals with public profiles who operate on Social Media without any, or only limited, forms of privacy settings being activated do so at their own risk. Often, Social Media sites will advise its users through its terms and conditions of the implications of not activating privacy controls, namely that all content they publish or share will be viewable by everyone, including sometimes people who, themselves, do not have an account with that provider.

4.4 Whilst the content or information shared by individuals on Social Media remains the property of that individual, it is nonetheless considered to be in the public domain. Publishing content or information using a public, rather than a private setting, means that the individual publishing it is allowing everyone to access and use that information, and to associate it with them.

4.5 The opposite of a public profile is a private profile. Some users of Social Media

will not wish for their content, information or interactions to be viewable to anyone outside of a very small number of people, if any. In these instances, users will normally set a level of privacy on their Social Media profiles that reflects what they are comfortable with being made available, meaning that, for example, only friends, family and other preapproved users are able to view their content or make contact with them through that site.

4.6 By setting their profile to private, a user does not allow everyone to access and use their content, and respect should be shown to that person's right to privacy under Article 8 of the Human Rights Act. This does not, however, extend to instances where a third party takes it upon themselves to share information which originated on a private profile on their own Social Media profile. For example, Person A publicises on their private Social Media page that they intend to throw a party, at which they will be selling alcohol and providing other forms of licensable activities, despite not having a licence from the Council to do so. Person B, who "follows" Person A's Social Media page, re-publishes this information on their public Social Media page. The information on Person A's profile cannot be used, however the same information on Person B's profile, can.

5 WHAT IS PERMITTED UNDER THIS POLICY

5.1 Whether or not Social Media can be used in the course of investigating an offence, or potential offence, will depend on a number of things, not least of which is whether the suspect has a Social Media presence at all. Investigating offences will always be a multi-layered exercise utilising all manner of techniques, and it is important not to place too high an emphasis on the use of Social Media in place of more traditional investigative approaches.

5.2 Further to this, a lack of information on an individual's Social Media profile should not be taken as evidence that something is or is not true. For example, a lack of evidence corroborating an individual's assertions that they were at a particular location on a specific day does not prove that they are being misleading and it is important to consider it only as part of a well-rounded investigation.

5.3 For those individuals who do have a presence on Social Media, a lot of what is permitted under this policy for use in investigations will depend on whether they have a public or private profile. As outlined in 4.4 above, where a person publishes content on a public profile, they allow everyone, including those not on that particular Social Media platform, to access and use that information whilst also allowing it to be associated with them.

5.4 In practice, this means that things such as photographs, video content or any

other relevant information posted by individuals and businesses to a public profile on any given Social Media platform can be viewed, recorded and ultimately used as evidence against them should the matter end in legal proceedings, subject to the usual rules of evidence.

5.5 When considering what is available on an individual's public Social Media profile, those investigating an offence, or potential offence, should always keep in mind what relevance it has to that investigation. Only information that is relevant to the investigation at hand, and goes some way toward proving the offence, should be gathered. If there is any doubt as to whether something is relevant, then advice should be sought from Legal Services.

6 WHAT IS NOT PERMITTED UNDER THIS POLICY

6.1 When it is discovered that an individual under investigation has set their Social Media account to private, Officers should not attempt to circumvent those settings under any circumstances. Such attempts would include, but are not limited to;

- sending "friend" or "follow" requests to the individual,
- setting up or using bogus Social Media profiles in an attempt to gain access to the individual's private profile,
- contacting the individual through any form of instant messaging or chat function requesting access or information,
- asking family, friends, colleagues or any other third party to gain access on their behalf, or otherwise using the Social Media accounts of such people to gain access, or
- any other method which relies on the use of subterfuge or deception.

6.2 Officers should keep in mind that simply using profiles belonging to others, or indeed fake profiles, in order to carry out investigations does not provide them with any form of true anonymity. The location and identity of an officer carrying out a search can be easily traced through tracking of IP Addresses, and other electronic identifying markers.

6.3 A distinction is made between one-off and repeated visits to an individual's Social Media profile. As outlined at paragraph 2 above, a RIPA authorisation must be sought in order to carry out directed surveillance against an individual. Whilst one-off visits, or otherwise infrequent visits spread out over time, cannot be considered "directed surveillance" for the purposes of RIPA, repeated or frequent visits may cross over into becoming "directed surveillance" requiring RIPA authorisation. A person's Social Media profile should not, for example, be

routinely monitored on a daily or weekly basis in search of updates, as this will require RIPA authorisation, the absence of which is an offence. For further guidance on this point, officers should contact a RIPA Authorising Officer.

6.4 Regardless of whether the Social Media profile belonging to a suspected offender is set to public or private, it should only ever be used for the purposes of evidence gathering. Interaction or conversation of any kind should be avoided at all costs, and at no stage should a Council Officer seek to make contact with the individual through the medium of Social Media. Any contact that is made may lead to accusations of harassment or, where a level of deception is employed by the Officer, entrapment, either of which would be detrimental and potentially fatal to any future prosecution that may be considered.

7 CAPTURING EVIDENCE

7.1 Once content available from an individual's Social Media profile has been identified as being relevant to the investigation being undertaken, it needs to be recorded and captured for the purposes of producing as evidence at any potential prosecution. Depending on the nature of the evidence, there are a number of ways in which this may be done.

7.2 Where evidence takes the form of a readable or otherwise observable content, such as text, status updates or photographs, it is acceptable for this to be copied directly from the site, or captured via a screenshot, onto a hard drive or some other form of storage device, and subsequently printed to a hard copy. The hard copy evidence should then be exhibited to a suitably prepared witness statement in the normal way.

7.3 Where evidence takes the form of audio or video content, then efforts should be made to download that content onto a hard drive or some other form of storage device such as a CD or DVD. Those CD's and/or DVD's should then be exhibited to a suitably prepared witness statement in the normal way. Any difficulties in downloading this kind of evidence should be brought to the attention of the Council's IT Team who will be able to assist in capturing it.

7.4 When capturing evidence from an individual's public Social Media profile, steps should be taken to ensure that all relevant aspects of that evidence are recorded effectively. For example, when taking a screenshot of a person's Social Media profile, the Council Officer doing so should make sure that the time and date are visible on the screenshot in order to prove when the evidence was captured. Likewise, if the evidence being captured is a specific status update or post published on the suspected offender's profile, steps should be taken to make sure that the date and time of that status update or post is visible within the screenshot. Without this information, the effectiveness

of the evidence is potentially lost as it may not be admissible in court.

7.5 Due to the nature of Social Media, there is a significant risk of collateral damage in the form of other, innocent parties' information being inadvertently captured alongside that of the suspected offender's. When capturing evidence from a Social Media profile, steps should be taken to minimise this collateral damage either before capturing the evidence, or subsequently through redaction. This might be particularly prevalent on Social Media profiles promoting certain events, where users are encouraged to interact with each other by posting messages or on photographs where other users may be making comments.

8 OTHER INFORMATION TECHNOLOGY TOOLS AVAILABLE FOR INVESTIGATIVE PURPOSES

8.1 Whilst Social Media can be a useful and fruitful means of investigating offences and potential offences, it is by no means the only tool available within the realm of Information Technology. A vast array of other, mostly web-based tools are also at the disposal of those conducting investigations. For example, where there is a website advertising the services of a local business, and there is evidence that this business is engaging in illegal activity, there are IT tools available that can track who is responsible for setting up that website, and so can be a good starting point when trying to link potential offenders to the offending business.

8.2 For assistance in identifying which tools may be appropriate, and how best to utilise them, advice should be sought from a RIPA Authorising Officer and or the Council's IT team.

9 RETENTION AND DESTRUCTION OF INFORMATION

9.1 Where recorded material (in any form or media) is obtained during the course of an investigation which might be relevant to that investigation, or another investigation, or to pending or future civil or criminal proceedings, then it should not be destroyed, but retained in accordance with the requirements of the Data Protection Act 2018 , the Freedom of Information Act 2000, and any other legal requirements, including those of confidentiality, and the Council's policies and procedures regarding document retention. Advice should be sought from the Information and Project Officer or the Monitoring Officer.

9.2 Personal data gathered by the Council is subject to the Data Protection Act 2018. When considering whether to retain the data, the Council should:

- review the length of time it keeps personal data;

- consider the purpose or purposes it holds the information for in deciding whether (and for how long) to retain it;
- securely delete information that is no longer needed for this purpose or these purposes; and
- update, archive or securely delete information if it goes out of date

9.3 Due to the nature of Social Media, it is important to remember that when information produced as a hard copy is destroyed in line with this paragraph, that all digital copies of that evidence is likewise destroyed.

10 REVIEW

10.1 This Policy will be reviewed periodically and in line with the Council's Code of Practice on Covert Surveillance to ensure that both documents remain current and compliant with relevant legal requirements and best practice guidance.