WIRRAL

POLICY AND PROCEDURE ON THE USE OF POWERS UNDER THE REGULATION OF INVESTIGATORY POWERS ACT

1. INTRODUCTION

1.1 ***"Surveillance plays a necessary part in modern life. It is used not just in the ~ targeting of criminals but as a means of protecting the public from harm and ~ preventing crime.*** "

From the Foreword to the Home Office's Code of Practice on Covert Surveillance

1.2 The use of covert surveillance by public authorities, particularly local authorities has been the subject of much recent debate. The use of covert surveillance is properly a matter of public concern. The purpose of this policy is to set out exactly how the Council will use its surveillance powers and comply with best practice.

1.3 **Councils may only use covert surveillance for the purpose of preventing or detecting crime and where doing so is in the public interest.** The Council uses covert surveillance to support its enforcement activities. It has been used principally by the officers in dealing with anti-social behaviour, flytipping and trading standards cases. This has resulted in many successful cases being brought which might otherwise not have been possible bringing rogue traders to account and improving the lives of Wirral residents suffering from severe anti-social behaviour and flytipping.

1.4 The Council approved a policy and procedure for the use of covert surveillance in 2004. The Council has been inspected six times by the Office of the Surveillance Commissioner in 2003, 2007, 2009, 2012, 2015 and 2018. The Policy and Procedure was amended in 2016 to take account of the monitoring of social networking sites and the possibility of non RIPA authorisations (paragraphs 9 and 10). It has been further revised in 2019 in order to incorporate the revised Codes of Practice published in August 2018 by the Home Office and the recommendations of the Inspector appointed by the Investigatory Powers Commissioner who visited the Council on 17 December 2018.

1.5 The Council is recommended to review and approve annually its policy and procedure for the use of covert surveillance.

2. RELEVANT LEGISLATION

2.1 **The Human Rights Act 1998 (HRA)**

2.1.2 The HRA gives effect to the rights and freedoms guaranteed under the European Convention on Human Rights and Fundamental Freedoms ("the Convention"). Article 8 of the Convention is relevant in the context of covert surveillance in that everyone has the right to respect for his/her private and family life, home and correspondence. It is now clear from decided cases that this right extends to activities of a professional or business nature and so includes employees. Article 6 of the Convention is relevant in the context of covert surveillance in that everyone has the right to a fair trial, including internal procedures or hearings, and fairness extends to the way in which evidence is obtained.

2.1.3 Consequently, there is to be no interference with the exercise of these rights by any public authority, except where:

Such interference is in accordance with the law and is necessary in a democratic society in the interests of:

- national security
- public safety
- the economic well-being of the country
- for the prevention of disorder or crime
- for the protection of health or morals
- the protection of the rights and freedoms of others.

The Council is a public authority. However, as mentioned above (and explained in more detail in section 3 below), local authorities may **only** undertake covert surveillance for the purpose of preventing or detecting crime.

2.1.4 The HRA can be found at:

www.opsi.gov.uk/ACTS/acts1998/19980042.htm

2.2 **The Regulation of Investigatory Powers Act 2000 ("RIPA")** (and associated Regulations)

2.2.1 RIPA was introduced shortly after the HRA to ensure that the use by public bodies of surveillance was codified. Prior to RIPA there was only limited regulation of the use by public bodies of surveillance. RIPA was passed to ensure a consistency of approach and to set in place safeguards to ensure that the use of surveillance is proportionate.

2.2.2 RIPA was passed well before the terrorism attacks on September 11 and was not introduced to deal with terrorism. RIPA and its associated regulations also follow the philosophy of recent legislation in trying to strike a balance between community responsibilities, including effective law enforcement, and individual rights and freedoms.

3.0 COVERT SURVEILLANCE

3.1 The term surveillance includes

- Monitoring, observing or listening to people, their movements, their conversations or their other activity or communication;
- Recording anything monitored, observed or listened to in the course of surveillance;
- Surveillance by or with the assistance of a surveillance device.

3.2 **Covert** surveillance is surveillance that 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. This needs to be contrasted with the deployment of **overt** surveillance. The use of such surveillance in places to which the public has access is increasingly commonplace. The Council has employed it in the form of CCTV monitoring of its offices, car parks and the town centres. CCTV monitoring is undertaken in accordance with the Council's Code of Practice for the operation of CCTV. CCTV is usually clearly marked through the use of signage. The Council must have regard to the Code of Practice on the use of CCTV published by the Secretary of State in June 2013.

3.3 RIPA applies where any covert surveillance of an identifiable or named person is carried out by a public authority carrying out an investigatory function. RIPA includes a local authority within the description of public authority.

3.4 Covert surveillance can be either

(a) **intrusive**, that is, carried out in relation to anything that is taking place on any residential premises or in any private vehicle by an individual or a surveillance device on the premises or in the vehicle; or

(b) **directed**, that is, undertaken for the purposes of a specific investigation or operation and involving the observation of a person or persons in order to gather information about them.

3.5 **Local authorities are <u>not</u> authorised to conduct <u>intrusive</u> surveillance**.

3.6 **Directed** covert surveillance that is likely to result in obtaining <u>private information</u> about a person is permitted by RIPA and its associated regulations **if** such surveillance has been authorised in the manner provided by the Act, the Home Office Code of Practice and the prescribed standard forms. Private information is any information relating to a person's private or family life. It includes the way in which a person conducts himself in his working life and also in a public place where there is a reasonable expectation of privacy e.g. two people holding a conversation in a street. It does not include publicly accessible information e.g. in a newspaper or on a website or public register nor does it include non verbal noise (e.g. music) or shouting which can be heard in the street or from adjoining property with the naked ear.

3.7 An authorising officer for a public authority may only grant authorisation to carry out directed surveillance if it is necessary in the interests of:

- national security (**not** applicable to local authorities);
- preventing or detecting crime;
- public safety (**not** applicable to local authorities);
- protecting public health (**not** applicable to local authorities);
- assessing or collecting any tax, duty, levy or other imposition, contribution or charge payable to a government department (**not** applicable to local authorities); or
- is specified by regulations.

3.8 **Local authorities may <u>only</u> authorise use of covert directed surveillance on the ground that it is necessary in the interests of <u>preventing or detecting crime or of preventing disorder</u>.** The use of surveillance must also be proportionate to what is being sought to achieve and a magistrates approval required as set out below.

3.9 From 1 November 2012 a magistrates approval will also be required for the Council's use of RIPA and will be in addition to the authorisation needed from an authorising officer. Magistrates may only grant approval for the use of covert directed surveillance where the criminal offence under investigation carries a maximum custodial sentence of six months or more except in relation to the offences of under age sales of alcohol and tobacco where this threshold will not apply. That restriction does not however apply to the use of covert human intelligence sources (see 4.0 below) or to the acquisition of communications data (see 5.0 below) where the offence need not carry a maximum custodial sentence. A magistrates approval is required both for an authorisation and for a renewal of an authorisation which has expired.

3.10 Authorisation is not required to record things which are not planned but arise as an immediate response to events. For example if an enforcement officer is attending a property to visit a witness and observes a neighbour causing criminal damage he/she can record covertly what they saw without authorisation.

3.11 Authorisation for covert surveillance is also not required where it is part of the general observation duties or activities of local authority officers and not part of a pre-planned surveillance of a specific person or group of people. An example would be Council officers attending a car boot sale where it is suspected counterfeit goods are being sold but no particular individuals are being targeted as likely suspects.

3.12 Particular care needs to be taken when the surveillance may give rise to the obtaining of **confidential information**. In this context confidential information means:

- Where legal professional privilege applies;
- Confidential personal information; or
- Confidential journalistic material

Legal professional privilege will apply to oral and written communications between a professional legal adviser and his/her client made in connection with the giving of legal advice or in connection with or contemplation of legal proceedings.

Confidential personal information is information held in confidence about a person's physical or mental health or to spiritual counselling or assistance. The information must have been created or acquired in the course of a trade, business or profession or for the purpose of any paid or unpaid office.

Confidential journalistic material includes material acquired or created for the purposes of journalism and held subject to an undertaking to hold it in confidence.

If the purpose of the surveillance is likely to obtain confidential information then this will need to be approved by the Director: Governance and Assurance and the Chief Executive. If in the course of an operation confidential material is obtained through surveillance this must be notified immediately to the Director: Governance and Assurance. It must be retained and provided to the inspector from the Investigatory Powers Commissioner at the next inspection.

3.13 An applying officer wishing to use directed surveillance must complete **FORM RIPADS1** (all forms are attached to this policy). The applying officer must fully complete all parts of the form. The officer should refer as necessary to the Home Office Codes of Practice, available on the internet.

3.14 The applying officer must consider the proportionality of the use of surveillance. The officer must consider the seriousness of the matter being investigated, the impact that any evidence obtained through the surveillance will have on the investigation and the level of intrusion which will be caused. The officer must take steps to ensure that any intrusion is kept to the minimum level necessary. Any intrusion in to the private life of persons not the subject of the investigation (e.g. family or visitors) should be minimised.

3.15 The completed form should be referred to an **authorising officer**. All Chief Officers may designate officers within their department as authorising officers for the purposes of RIPA. On receipt of the form the authorising officer will contact the Director: Governance and Assurance to obtain a unique reference number. The authorising officer must be a Director or Head of Service or Service Manager. The authorising officer will place the form on the central register. The register is an electronic folder with access rights limited to authorising officers (for their area only) and the Director: Governance and Assurance or his/her nominated representatives (to all contents). When an authorising officer places a form on the register he/she will also separately notify the Director: Governance and Assurance by e-mail that this has been done. If the authorising officer does not have access to the register he or she will e-mail the form to the Director: Governance and Assurance who will arrange for it to be placed on the register. All forms for authorised

applications shall be placed on the register immediately. All applications shall remain on the register for at least 3 years. Officers should ensure that when they complete the authorisation forms they comply with the following requirements:

(a) the information on which an investigation is based must be clearly identified

(b) applications should state clearly why the covert activity is believed to be necessary and proportionate and why other methods of obtaining information are not feasible or practicable.

(c) Authorising Officers should clearly state why they consider the covert activity is necessary and proportionate (including the steps to be taken to minimise intrusions into privacy, particularly of those persons not suspected of crime or disorder). They must never be granted retrospectively.

(d) Authorising Officers must describe accurately all the covert activity which they are authorising so as to ensure that the limits are not infringed.

(e) Technical feasibility studies should be presented to the Authorising Officer along with the application for authorisation. They should be attached to the authorisation. If the authorisation is granted, the person carrying out technical installations (e.g. of cameras and sound recording equipment) must see the relevant parts of the authorisation prior to the installation of any surveillance equipment.

(f) Review dates should be stipulated by Authorising Officers at the time they authorise the covert surveillance for any extended period. This is to ensure that the need for continuation of the surveillance is regularly assessed and recorded on Form RIPADS2 and that (where appropriate) authorisations are either renewed (before they expire) on Form RIPADS4 or cancelled on Form RIPADS3.

(g) Cancellations of authorisations should be made promptly when the need for covert surveillance has ceased. The cancellation should contain a full description of the activity which has been authorised, what the results of the surveillance were, and how and when any products of the surveillance will be stored, retained or destroyed.

(h) The designated authorising officers are currently Mike Cockburn (Lead Commissioner: Environment and Community Services), Caroline Laing (Constituency Manager), and Mark Camborne (Strategic Commissioner for Environmental and Community Services). They have delegated authority to apply to the magistrates for approval of covert surveillance and to authorise named officers to make such applications on behalf of the Council. They also have delegated authority to authorise covert surveillance in the circumstances set out in paragraph 10 (non RIPA authorisations).

3.16 **Urgent Oral Applications**

3.16.1 It is no longer possible to grant urgent oral authorisations. All authorisations have now to be in writing and approved by a magistrate.

3.17 **Review/Cancellation**

3.17.1 Written authorisations will lapse automatically unless they are renewed after **3 months**. However, authorisations should be reviewed on a regular basis and cancelled when they are no longer required for the purpose for which they were granted. In each case the authorising officer within each public authority should determine how often a review should take place. This should be as frequently as is considered necessary and practicable. On carrying out a review the authorising officer should complete a **Form RIPADS2**. Once completed the form should be placed on the central register immediately either by the authorising officer directly or via the Director: Governance and Assurance. If the form is placed directly on the register the authorising officer must notify the Director: Law and Governance that this has been done by e-mail.

3.17.2 If upon review the need for directed surveillance no longer exists then the authorisation will be cancelled immediately. On cancellation the authorising officer shall complete **Form RIPADS3**. The completed form shall be placed on the central register either by the authorising officer directly or via the Director: Governance and Assurance. If the form is placed directly on the register the authorising officer must notify the Director: Governance and Assurance that this has been done by e-mail.

3.18 **Renewal**

If the authorisation is due to lapse it may be renewed for a period of a further 3 months provided the need for the surveillance continues. If a renewal is required a **Form RIPADS4** shall be completed. If an authorisation is renewed for a further period of 3 months it should be reviewed during that period. All renewals will require the approval of a magistrate.

3.19 **Audit Checks**

The Director: Governance and Assurance shall carry out a regular audit of authorisations contained on the central register at least once every 3 months.

3.20 **Code of Practice**

The Home Office Codes of Practice on the Use of Covert Surveillance can be viewed at: http://security.homeoffice.gov.uk/ripa/publication-search/general-publications/ripa-cop/index.html

3.21 The following examples illustrate the circumstances in which it is necessary and appropriate to obtain authorisation for covert surveillance:

3.21.1 Residents report to the Anti-social Behaviour Team that the occupants of a neighbouring property are disturbing them at night by engaging in noisy parties or quarrels fuelled by the consumption of alcohol and threaten them with violence when they protest.

In such circumstances covert surveillance (e.g. by means of a camera and sound recording devices unobtrusively fitted to an adjoining property) would be necessary to prevent crime and disorder (because witnesses are likely to be intimidated by the threat or use of violence) and proportionate (the disturbance is frequent and at a high level). The recording device must not be capable of picking up conversations at a normal level within the home targeted (and consequently is not intrusive). The Authorising Officer must therefore have available a technical feasibility study.

The amount of collateral intrusion on the privacy of the persons should be low (if the device is directed only at the targeted property) and if the need for continual surveillance is regularly reviewed by the Authorising Officer to ensure that the recording device is removed (when, for example it becomes apparent that the antisocial behaviour has ceased or significantly diminished) Those fitting the recording device must be shown that part of the authorisation which defines the permitted coverage of the camera so that the limits of the authorisation are not infringed.

3.21.2 The police approach the operators of the Council's CCTV cameras and ask them to train their cameras on a particular part of a public place where they suspect drug dealers are doing business. Council staff may only comply with the request of the police if they are satisfied that the police officers have obtained the necessary authorisation for directed surveillance from their superiors. Whilst the cameras are overt, they would be used for the purposes of a specific investigation or specific operation and therefore that use would require authorisation. Members of the public would not normally expect public cameras to be trained on specific individuals or on specific public places for protracted periods and therefore their use in that instance would be covert. The same principles would apply if Trading Standards Officers requested the use of CCTV cameras to monitor the activities of suspected illegal traders in a prohibited street. Authorisation for directed surveillance would be required before the CCTV cameras could be used for that purpose.

3.22 The Director: Governance and Assurance will compile and maintain electronically a central record of authorisations granted by authorising Officers. That central record shall contain the following information about the authorisation:

(a) Whether it is for Directed Surveillance or Covert use of Human Intelligence Source.

(b) Its unique reference number.

(c) Applicant's name and title.
(d) Department and Section.

(e) Identity of Target and the title of the investigation.

(f) Date of authorisation.

(g) Renewal Date and name and/or title of Authorising Officer.

(h) Review Date.

(i) Whether the investigation is likely to result in obtaining confidential information.

(j) Date of approval by magistrate of authorisation/renewal.

(k) Cancellation Date.

The information contained in the Central Record will be used by the Director: Governance and Assurance to monitor the use by departments of RIPA. It will be a standing item on the agenda of the quarterly meetings of the Coordinators Group referred to in paragraph 7.1.

3.23 The Director: Governance and Assurance has been appointed the Senior Responsible Officer to perform the duties of that office set out in the Home Office Codes of Practice. These include liaising with IPCO Inspectors and taking steps to ensure compliance with RIPA and the Codes by authorising officers.

4.0 COVERT HUMAN INTELLIGENCE SOURCES (CHIS)

4.1 The use of CHISs is also regulated by RIPA. A CHIS is a person who establishes or maintains a relationship with someone in order to obtain information, to provide another person with access to information or to disclose information as a consequence of that relationship. Should an officer consider the use of a CHIS as necessary, they must liaise with the Director: Governance and Assurance. If the use of a CHIS is deemed necessary, special arrangements will be made for their use in accordance with the Home Office Code of Guidance on Covert Human Intelligence Sources (see paragraph 4.5 below). It is not anticipated that CHISs will be used often by the Council. However, if professional witnesses are used they may fall within the definition of CHISs. Only the Chief Executive can authorise the use of a CHIS, if it will involve the likely disclosure of confidential information or the use of juveniles.

4.2 If an investigating officer does believe that the use of a CHIS is necessary in the course of an investigation he/she should complete **FORM RIPACHIS1**. The officer must consider the safety and welfare of a person acting as a source and must carry out a risk assessment before authorisation is granted. The use must be proportionate to what is intended to be achieved. The authorisation will lapse automatically if not renewed after a period of **12 months**.

4.3 It should be borne in mind that a person can become a covert human intelligence source if he regularly supplies information to the Council without being asked to do so provided he obtains the information by virtue of his personal relationship with the suspect or his associates and not for example by merely noting down passively evidence of crime or disorder as a member of the public. In such circumstances legal advice should be sought before acting on the information received from the informant.

4.4 Special considerations apply if the person to be used as a source is **vulnerable** or a **juvenile**. In such circumstances advice should be sought

from the Director: Governance and Assurance. Authorisation may only be granted by the Chief Executive, as Head of Paid Service.

4.5 The same procedures outlined above in respect of directed surveillance of:

- Maintenance of a central register
- Confidential information
- Review
- Cancellation
- Renewal; and
- Audit checks

Shall also apply to the use of CHISs. The following forms shall be used **FORM RIPACHIS2** (review), **FORM RIPACHIS3** (cancellation) and **FORM RIPACHIS4** (renewal)

4.6 The following examples illustrate the circumstances in which it is necessary and proportionate to obtain authorisation for the use of a CHIS (Covert Human Intelligence Source).

4.6.1 The Anti-Social Behaviour Team engage a private detective to pose as a tenant of Leasowe Community Homes in order to form a relationship with a group of tenants suspected of committing acts of serious anti-social behaviour, including criminal damage to property, drug dealing and intimidation of other tenants. The purpose of establishing a relationship is to obtain information admissible in possession proceedings (e.g. by covert tape recordings of conversations) or to assist the police or the Anti-Social Behaviour Team to anticipate the future criminal behaviour of the tenants under suspicion. No potential witnesses are willing to co-operate with the Anti-Social Behaviour Team by installing cameras in the properties. Authorisation would be required in such circumstances since the private detective will be establishing a personal relationship with the subjects to obtain and disclose information to the Anti-Social Behaviour Team in a manner that is calculated to ensure that the subjects are unaware of the purpose of the personal relationship. This example also illustrates the difficulties, dangers (and expense) of using a CHIS in the circumstances where evidence cannot be obtained by other methods.

4.6.2 A trading standards officer enters a shop and makes a “test purchase” from a retailer suspected of selling “counterfeit goods”. No authorisation would be required for a CHIS because he would not be establishing a personal relationship with the retailer (although if he had attached to his person a concealed camera it would be necessary for him to obtain authorisation for directed surveillance). If on the other hand, the trading standards officer struck up a conversation with the retailer whilst posing as a member of the public in order to ascertain whether the retailer (without any encouragement from the Trading Standards Officer) would offer to sell him (or another customer) counterfeit goods, then he would be acting as a CHIS and authorisation would be required. The essence of a CHIS is that he obtained information by winning someone’s confidence on a false basis

4.6.3 If, however, a juvenile were used to make a test purchase of alcohol from a shopkeeper (suspected of under age sales) in the presence of an adult Trading Standards Officer, a directed covert surveillance authorisation would be required because the shopkeeper would not be aware of the covert observations being made by the officer. It would also be required if a concealed camera were used.

4.6.4 The Anti-Social Behaviour Team regularly receives information from a member of the family of a suspected perpetrator who volunteers to provide evidence without being requested to do so. The informant is performing the function of a CHIS if the information has been obtained as a result of the family relationship.

4.7 **Code of Practice**

The Code of Practice relating to the use of CHISs can be found at: http://security.homeoffice.gov.uk/ripa/publication-search/general-publications/ripa-cop/index.html

5.0 COMMUNICATIONS DATA

5.1 Requests for communications data will be dealt with by **designated persons**. Those persons who are authorising officers for the purposes of directed surveillance and CHISs shall also be designated persons for the purposes of obtaining communications data. There must be a **Single Point of Contact (SPOC)**, to whom applicants must submit their requests for communications data. This is to ensure there is a specific point of accountability in each authority requesting data for reasons connected with RIPA and the HRA etc. The SPOC for the Council is the organisation known as NAFN (The National Anti Fraud Network)

5.2 It is important to note that we are not referring here to the interception of communications or the **content** of communications. The Council does not have power to intercept communications or acquire content. From 5/2/19 the law is now set out in the Investigatory Powers Act 2016(IPA 2016) and the Data Retention and Acquisition Regulations 2018

5.3 There are 2 types of communications data;

- "Events Data" being telecommunications data that identify or describe an event consisting of one or more entities engaging in a specific activity at a specific time e.g traffic and service use data;and

- "Entity Data" being data which identify or describe a person or thing in its association with a telecommunications system e.g subscriber data.

5.4 More information on what constitutes these types of communication data is set out in the Home Office Code of Practice (see paragraph 5.9 below).

Published in November 2018. Advice can also be sought from the Director: Governance and Assurance. Local authorities are only able to seek disclosure under RIPA of service use data, traffic data and subscriber data **not** of internet connection records.

5.5 Applications may be made for data e.g. itemised bills or subscriber data e.g. whether a person uses a particular network, who is the user of a particular number. A request for such information can only be made where it is necessary for the purpose of preventing or detecting crime or preventing disorder.It must also be necessary for the purposes of a specific investigation or operation and if the request is for "Events Data" it must also be for the purpose of preventing or detecting "serious crime"(e.g offences by corporate bodies,offences attracting a maximum prison sentence of at least 12 months,or conduct involving the use of violence or which results in substantial financial gain or by a large number of people in pursuit of a common purpose or a breach of a person's privacy or the sending of a communication). The request must be proportionate.

5.6 The form for completion for disclosure of communications data including guidance on completion is attached as **FORM RIPACD 1**.Applications must be made to the Investigatory Powers Commissioner (IPCO) through NAFN with the prior consent of the Council's SRO for approval of the proposed authorisation.The IPC has delegated this function to his staff in the Office for Communications Data Authorisations (OCDA). An authorisation or notice remains valid for up to **one month**. A valid authorisation or notice may be renewed for a further period of up to one month.

5.6 An authorisation or notice must be cancelled as soon as it is no longer necessary for the service provider to comply with the notice or the conduct required by the notice is no longer proportionate to what was sought to be achieved.

5.7 The **Senior Responsible Officer(SRO)** must be responsible for:

- the integrity of the process in place within the public authority to acquire communications data;
- compliance with the relevant legislation and with this code;
- oversight of the reporting of errors to the Investigatory Powers Commissioner (IPCO) and the identification of both the cause(s) of errors and the implementation of processes to minimise repetition of errors;
- engagement with the IPCO inspectors when they conduct their inspections; and
- where necessary, overseeing the implementation of post-inspection action plans approved by the Commissioner.

In Wirral the Senior Responsible Officer is the Director: Governance and Assurance.

5.8 In Wirral there has been very limited use of these powers and none since 2015.

5.9 The Home Office Code of Practice on the use of Communications Data can be viewed at: http://security.homeoffice.gov.uk/ripa/publication-search/ripa-cop/acquisition-disclosure-cop.pdf

6.0 REPORTING AND REVIEW

6.1 The Council recognises the public interest in the use by it of these powers. It is essential that it regularly monitors and reviews the use of these powers. Therefore, this policy and procedure shall be subject to a review on at least an annual basis. The Director: Governance and Assurance shall report quarterly to the Audit and Risk Management Committee in accordance with the Codes of Practice on the use of RIPA and annually in respect of the need for any revisions to this policy and procedure.

7.0 COORDINATION AND TRAINING

7.1 All Departments that use or may use the Council's powers under RIPA shall nominate a Departmental Coordinator under this Policy. The Departmental Coordinators (or their nominees) shall meet at least once a quarter to review the operation of this policy, share best practice and consider training needs. Those meetings shall be chaired by the Director: Governance and Assurance or his/her nominated representative. The departmental co-ordinators and authorising officers are listed in paragraph 3.14(h). That list may be amended from time to time as new Directors and Heads of Service are appointed. The current list can be obtained from the Director: Governance and Assurance.

7.2 The Council shall ensure that adequate training is provided to officers in the use of the powers. A training register shall be maintained and all authorising/designated officers will receive training at least every 2 years. A copy of the register can be obtained from the Director: Governance and Assurance. If an authorising/designated officer has not attended any training for a period of 2 years they shall **automatically cease** to be a responsible/authorised officer.

8.0 APPLICATIONS TO A MAGISTRATE FOR APPROVAL OF RIPA AUTHORISATIONS AND RENEWALS

8.1 These are governed by Rules 6.27 and 6.28 of the Criminal Procedure Rules 2012 (SI2012 No. 1726). No court fee is currently payable.

8.2 Home Office Guidance on local authority applications for approval by Magistrates was given in October 2012 and may be viewed on the Internet.

8.3 Annex B of the Home Office Guidance contains a model application form and a model form of order by the magistrates. These forms should be used when applying to a magistrate.

8.4 Paragraphs 84 to 98 of the Home Office Guidance set out the procedure. Applications should be made by investigating officers designated by the Authorising Officer. The hearing will be in private. The authorisation must be completed in sufficient detail to make the case for approval by itself without the need for additional oral evidence.

8.5 The Magistrate should record his/her decision on the form of order and retain a copy of the RIPA authorisation. He/she must be satisfied that there are reasonable grounds to believe the authorisation or renewal was both necessary and proportionate and continues to be so at the hearing. He/she must also be satisfied that the person within the Council granting the authorisation was of sufficient seniority by holding a post described in paragraph 3.14. A certificate signed by the Council's Monitoring Officer should be produced for that purpose verifying the identity of the person granting the authorisation and the post he or she holds.

9.0 SOCIAL NETWORKING SITES AND RIPA

9.1 During the course of an investigation into a possible criminal offence falling within paragraph 3.9 above, officers may view what persons have said on various forms of social media eg Twitter, Facebook.

9.2 No prior authorisation of directed covert surveillance will usually be required if the person's communications are to the world at large (ie open source) because there can be no reasonable expectation of privacy in such cases. Repeat viewing of open source sites, without the knowledge of the person, for the purpose of intelligence gathering for a specific investigation will, however, constitute directed surveillance and will require prior authorisation because the degree of surveillance and its purpose would be covert and unexpected.

9.3 No prior authorisation of the use of a covert human intelligence source would be required if the officer made no attempt to win the person's confidence on a false basis eg by falsely posing as a potential friend nor would simple preliminary reconnaissance of a site require directed covert surveillance authorisation if the intent were to establish whether the contents were of interest and there was no subsequent systematic recording of information about a particular person or group of persons for the purpose of a criminal investigation. Similarly viewing open source sites in order to update information obtained by preliminary reconnaissance would not be covert surveillance but part of an officer's general observational duties.

9.4 If however the conditions in 9.3 do not apply then the appropriate authorisation under RIPA would be required in liaison with the police where they have an interest in the outcome of the investigation.

9.5 An example of the need for directed surveillance authorisation would be repeat viewing and recording of information on open source sites to determine whether a sex offender was visiting a household that contained children at risk of significant harm. In such circumstances authorisation for directed covert surveillance would be for the purpose of preventing serious offences against children by gathering evidence for use in care proceedings brought to protect them from harm.

10.0 COVERT SURVEILLANCE WHEN RIPA AUTHORISATIONS ARE NOT AVAILABLE

10.1 It is not possible to use RIPA authorisations when surveillance by a local authority is required not for one of its core statutory functions but for an ancillary function (eg disciplinary proceedings against an employee suspected of theft).

10.2 Equally as explained above RIPA authorisation is not available if the purpose of the covert surveillance is not to detect a criminal offence falling within paragraph 3.9 above, but to further some other legitimate aim eg to monitor the household of a family whose children may be at risk of significant harm by the covert visits of a person whose presence is reasonably believed to be detrimental to the children's welfare, but where the risk of harm is emotional

and not of physical violence and therefore no criminal offence is apprehended.

10.3 In such circumstances covert surveillance that is repeated and systematic will only be lawful if it is carried out in accordance with the fair processing of personal data provisions of the Data Protection Act 2018 (DPA). In particular:

10.3.1 Legal advice must first be obtained.

10.3.2 A privacy impact assessment must be carried out by using the RIPA form for authorising directed surveillance.

10.3.3 The privacy impact assessment must identify the adverse impact on privacy of any person and enable the authorising officer to determine whether the aim of the covert surveillance is legitimate, and whether such surveillance is necessary and proportionate to achieve that aim having regard to the importance of its purpose, the adverse effect on the privacy of persons, and the possibility of using other less intrusive methods of investigation.

10.3.4 Any applicable guidance from the Information Commissioner eg the Employment Practices Code should be followed.

10.3.5 Only authorising officers are authorised to approve such covert surveillance which is outside the scope of RIPA.

10.3.6 A record of any such approved non RIPA covert surveillance must be submitted promptly to the Senior Responsible Officer together with a summary of the outcome. The Senior Responsible Officer shall include such authorisations in his regular reports to the Audit and Risk Management Committee.

11. GOOD PRACTICE IN RELATION TO THE OBSERVATION OF OPEN SOURCE SOCIAL MEDIA SITES

11.1 In each Council department the RIPA coordinator should designate a limited number of officers who are trained in RIPA, DPA and HRA. The RIPA coordinator is authorised to open an overt Facebook profile or account. Officers should never use their own Facebook profiles. Only the trained officers are permitted to research social media.

11.2 All requests for research on social media must be referred either to the RIPA coordinator or the trained officers who would decide whether the research required either RIPA or non RIPA authorisation (under the DPA or HRA) by an Authorising Officer. If there is any doubt advice should be sought from an Authorising Officer who in turn may seek legal advice from the Senior Responsible Officer (SRO) or his solicitors.

11.3 A written log of each use of social media by the RIPA coordinator or by the designated trained officers must be made which records who authorised whom to do what, when, why and how. In particular their rationale for using or monitoring social media must always be recorded.

11.4 Those written logs must be made available to the SRO upon request so that their contents can be discussed at the Coordinators meetings. Those written logs will be stored centrally by the SRO.

11.5 If practicable the trained officers should alert a subject to the fact that their social media will be examined in order to ascertain eg whether they are complying with a court order or with promises they have made to the Council (eg arrangements for contact with a child in need of protection). That will make any surveillance overt and outside RIPA and easier to justify under the DPA and the HRA.

12. SECURITY AND RETENTION OF PERSONAL DATA DERIVED FROM RIPA INVESTIGATIONS

12.1.SECURITY FROM UNAUTHORISED ACCESS

(a) CCTV images.

(i) The manager shall designate those persons who shall have access to retained images being only those who have a need to know i.e. those closely involved in the investigation.

(ii)The images must be secured against unauthorised interference and editing by being stored securely and labelled in Council premises to which access is restricted. Records Management could offer that facility.

(iii)The images should only be capable of being viewed in Council premises not in an employee's home.

(iv) Disclosure to 3rd parties e.g. the police should (in the absence of a court order) only be authorised by a RIPA Co-ordinator or Authorising Officer and be for the purpose of preventing or detecting crime or for the purpose of legal proceedings. Such disclosures must be recorded in writing and be capable of being justified after a data protection impact assessment has been carried out which weighs in the balance intrusions into a person's privacy against the objective of crime prevention and detection. The authorisation should stipulate the period during which the personal data may be retained before destruction.

(b)Other records of investigations.

(i) To the extent that they include personal data ,such records should only be accessible to those persons who have a need to know being those closely involved in the investigation and be the minimum necessary for the purpose of detecting or preventing crime or for the conduct of legal proceedings.

(ii)Disclosures to 3rd parties should only be allowed in the circumstances set out in 1(a)(iv) above

.

(iii)Copying and transmission of personal data (pathways) should be limited to what is strictly necessary for the purposes of the investigation. The manager should

identify those pathways and be able to demonstrate that each one was necessary and could not have been eliminated. The more pathways there ar , the greater the risk of unauthorised access. Managers should consider the advantages of storing RIPA records on Microsoft TEAMS with access restricted to those employees who are closely involved in the investigation.

(iv) Electronic files containing personal data should be password protected or encrypted and access limited to those persons who have a need to know .A display of personal data on a computer screen should only take place in a setting in which no unauthorised person is present e.g. not in an open plan office or in a room at home to which other members of the household have access or are present.

(v)Paper files containing personal data should be stored securely in locked cupboards or cabinets on Council premises and not in an employee's home or vehicle and be accessible only to those employees authorised by the RIPA co-ordinator who are closely involved in the investigation.

(vi) Staff should follow the Council's security procedures as set out in its general policies on data protection.

12.2.RETENTION AND DESTRUCTION.

(a) CCTV images.

(i) Images should not be retained for longer than is necessary to fulfil the purpose of preventing or detecting crime or for disclosure in legal proceedings including the requirements of the code of practice issued under the Criminal Procedure and Investigations Act 1996 which requires retention of all material relevant to a criminal investigation.

(ii)Subject to the above, images of persons whose privacy has been the subject of inadvertent interference should be destroyed within a month of being recorded.

(iii)Images should be destroyed as soon as the purposes in 2(a)(i) have been achieved by making access to them impossible. This will usually be no later than one month after the end of the investigation. If there has been a prosecution, however, images should be securely retained until 6 years have elapsed since the conclusion of the case or immediately thereafter if the data subject has been acquitted and there is no prospect of an appeal. Compliance is the responsibility of the RIPA co-ordinator who should carry out and record in writing monthly reviews of the necessity of retaining CCTV images.

(b)Other records containing personal data.

(i)The above procedures should also be applied to other records of personal data save that the reviews by the RIPA co-ordinator of the need to retain personal data should be conducted at not more than 6 monthly intervals and take account of legal constraints on destruction e.g.in relation to child care and adoption records. Records of RIPA investigations should only be retained if retention would enable the welfare of the child to be better safeguarded. Personal data relating to persons outside the child's family should generally be destroyed unless it concerned an investigation into possible abuse.

(ii)The outcomes of the 6 monthly reviews should be recorded in writing and made available to the Senior Responsible Officer (the Council's Monitoring Officer or the solicitor to whom he has delegated day to day management of RIPA).

(iii)Any problems concerning the reviews should be discussed at the quarterly meetings of RIPA Co-ordinators.

DATE 28 JUNE 2021