Kettering Borough Council

Investigation and Enforcement Surveillance Applications

Policy and Procedures

Updated - Nov 2018

Contents

INTRODUCTION

1.0 Purpose, Intent and Extent

1.1 This Policy is intended to formalise the ways in which Kettering Borough Council (KBC) will comply with the Human Rights Act 1998 (HRA) and the Regulation of Investigatory Powers Act 2000 (RIPA) with regard to the deployment of covert surveillance techniques.

1.2 Article 8 of the Human Rights Act 1998 provides rights of respect for private and family life, home and correspondence. RIPA ensures that public bodies comply with their obligations under the HRA and can demonstrate that they have done so.

1.3 It is important that officers involved in enforcement and investigations are fully appreciative of the fact that they are not subject to RIPA when undertaking their normal day to day activities e.g. wardens on patrol. It is perfectly permissible for officers engaged in this kind of activity to observe what is going on in their 'patch' and to record instances or events where evidence is required or intelligence is being gathered. RIPA only comes into play when specific individuals are being investigated in connection with a specific enquiry and the observations or indeed surveillance, takes on a more systematic and covert nature.

1.4 Under RIPA, a public authority can only interfere with a person's Article 8 rights if it can be shown that the interference had a clear legal basis, which in the case of Local Authorities can only be in connection with the prevention and detection of 'serious' crime and/or the prevention of disorder; that the interference is necessary and proportionate to aims of the enquiry and/or the information being sought could not have been obtained by less intrusive means - (see para 1.8).

1.5 In addition, when applying for or authorising applications under RIPA, Officers of the Council will have regard to any statutory codes of practice which apply.

1.6 The Council could use surveillance in several areas of operation e.g. fraud investigation and environmental and planning enforcement, housing, licensing etc. – it is important therefore that any surveillance undertaken complies with the legislation and is undertaken in accordance with the approved procedures.

1.7 That said, even when RIPA authorisation is not required, persons employed by KBC, when conducting activities which include surveillance, will still be required to record their reasons for not seeking authorisation under RIPA, in order to demonstrate that they have afforded the appropriate respect for a persons private and family life as required under Article 8 of HRA.

1.8 From 1 November 2012 there have been significant changes in the legislation as it applies to Local Authorities. From that date, if officers of any Local Authority wish to deploy Directed Surveillance, they can only do so if the suspected criminal offence attracts a maximum custodial sentence of 6 months or more or the offence is a criminal offence relating to the underage sale of tobacco or alcohol.

1.9 Another change effective from 1 November 2012 is that once an application has been authorised by the Authority it will then be subject to section 37 and 38 of the Protection of Freedoms Act 2012. This will require the Authority to obtain an order approving the granting of the authorisation, or renewal of an existing authorisation from a Justice of the Peace, be it a District Judge or lay magistrate. This process will be outlined later in the policy.

1.10 In accordance with the Regulation of Investigatory Powers (Directed Surveillance and Covert Human Intelligence Source Surveillance) Order 2003, the Council has nominated specific officers to authorise or sanction the use of covert surveillance, these being the posts as listed in Appendix 1 of this Policy and the Council will ensure that all Officers who are involved in surveillance and granting of authorisations are aware of the procedures to be followed, and that appropriate training is given.

1.11 In conclusion the principles that need to be adhered to are that:

- **Not all surveillance requires RIPA authorisation**
- **Some surveillance can be undertaken without RIPA authorisation**

  But

- **RIPA authorisation MUST be obtained for Directed Surveillance**
- **In ALL cases consider proportionality, collateral intrusion and whether or not the same information could be obtained in a less invasive manner**

ALL surveillance conducted for or on behalf of KBC requires management authorisation, then approval by a Justice of the Peace

IF it is Directed Surveillance, the activity can only be conducted where the suspected criminal offence attracts a maximum custodial sentence of 6 months or more

OR the offence is a criminal offence relating to the underage sale of tobacco or alcohol.

2.0 Relevant Definitions

Before detailing the procedures officers will follow when conducting surveillance as part of their investigations, it will be helpful to list the relevant definitions:

'Surveillance' includes monitoring, observing or listening to persons, their movements, conversations or other activities and communications. It may be conducted with/without the assistance of a surveillance device and includes the recording of any information obtained.

General observation' forms part of the duties of many law enforcement agencies and other public authorities and is not usually regulated by RIPA. Indeed the police and other public authorities do not need to seek a RIPA authorisation just because they are going to use covert techniques, only when the techniques are likely to result in the acquisition of information relating to a person's private or family life. See page 6 for the definition of 'Private Information'.

'Covert surveillance' means surveillance that is, **and only if it is**, carried out in a manner calculated to ensure that the person subject to the surveillance is unaware that it is or may be taking place.

'Overt surveillance' means surveillance that is carried out without being secretive or clandestine and which is therefore essentially open and something which the/any possible subject of the surveillance is aware of.

'Directed Surveillance' means surveillance which:

a) is **covert** but not intrusive surveillance; **and**

b) is undertaken for the purpose of a specific investigation or a specific operation; **and**

c) it is likely to result in the obtaining of private information about a person (whether or not one specifically identified for the purposes of the investigation or operation); **and**

d) it is conducted otherwise than by way of an immediate response to events or circumstances the nature of which are such that it would not be reasonably practicable for an authorisation to be sought for the carrying out of the surveillance.

If an immediate response is appropriate in such circumstances then the observation made would not constitute Directed Surveillance.

'Intrusive Surveillance' means **covert** surveillance carried out in relation to anything taking place on residential premises or in any private vehicle and that involves the presence of an individual on the premises or in the vehicle or is carried out by means of a surveillance device. This kind of surveillance may take place by means either of a person or device located inside residential premises or a private vehicle of the person who is subject to the surveillance or by means of a device placed outside which consistently provides a product of equivalent quality and detail as a product which would be obtained from a device located inside. See Page 6 for definition of 'Residential Premises.'

Surveillance within the ambit of the Regulation of Investigatory Powers (Extension of Authorisation Provisions: Legal Consultations) Order 2010 (SI2010/461) is to be treated as intrusive surveillance. This extends the provision to include places of imprisonment or detention, remand or committed in custody for trial or sentence; detention under paragraph 16(1), (1A) or (2) of Schedule 2 or paragraph 2(2) or (3) of Schedule 3 to the Immigration Act 1971 or section 36(1) of the UK Border Act 2007; detention under Part VI of the Criminal Procedure (Scotland) Act 1995, the Mental Health (Care and Treatment) (Scotland) Act 2003 or the Mental Health Act 1983; police stations; the place of business of any professional legal adviser; and any place used for the sittings and business of any court, tribunal, inquest or inquiry.

A local authority <u>cannot</u> undertake Intrusive Surveillance.

'Private vehicle' means any vehicle, including vessels, aircraft or hovercraft, which is/are used primarily for the private purposes of the person who owns it or of a person otherwise having the right to use it. This would include, for example, a company car owned by a leasing company and used for business and pleasure by the employee of the company.

'Residential premises' means so much of any premises as is for the time being occupied or used by any person, however temporarily, for residential purposes or otherwise as living accommodation (specifically including hotel or prison accommodation that is so occupied or used). Common areas, such as hotel dining areas or communal stairways in blocks of flats, to which a person has access in connection with their use or occupation of that accommodation, are specifically excluded.

'Private information' means any information relating to a person in relation to which that person has or may have a reasonable expectation of privacy. This includes information relating to a person's private or family life and this should be considered to include an individual's

private or personal relationship with others and family life should be construed as extending beyond the formal relationships created by marriage, including business and professional relationships. A person's private life may be affected by surveillance affected outside their home, business or other premises**.** A person's reasonable expectation as to privacy is a significant consideration albeit not necessarily a conclusive factor.

Private life considerations are likely to arise if several records are to be analysed together to establish, for example, a pattern of behaviour, or if one or more pieces of information (whether or not available in the public domain) are covertly (or in some cases overtly) obtained for the purpose of making a permanent record about a person or for subsequent data processing to generate further information. In such circumstances, the totality of information gleaned may constitute private information even if the individual records do not and where such conduct includes any form of surveillance, a Directed Surveillance authorisation will be required.

'Proportionality.' This means that the person granting the authorisation must believe that the use of the surveillance is proportionate to what is sought to be achieved by the conduct and use of that activity.

This involves balancing the intrusiveness (invasiveness) of the use of the surveillance on the target and others who might be affected by it against the need for the surveillance to be used in operational terms. The use of surveillance will not be proportionate if it is excessive in the circumstances of the case or if the information which is sought could reasonably be obtained by other less intrusive means. The use of surveillance must be managed and not used unfairly or in an arbitrary manner.
As applicants need to evidence all of this on the surveillance application forms be they for Directed or some other form of surveillance, Authorising Officers need to ensure that they have considered all the aspects of proportionality before they authorise.

This can be done by:

- balancing the size and scope of the proposed activity against the gravity and extent of the perceived crime or offence;

- explaining how and why the methods to be adopted will cause the least possible intrusion on the subject and others;

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

- evidencing, as far as reasonably practicable, what other methods

had been considered and why they were not implemented.

'Collateral intrusion' means intrusion into the privacy of those not the subject of or otherwise directly connected with the surveillance by obtaining private information about them. Where it is proposed to conduct surveillance activity specifically against individuals who are not suspected of direct or culpable involvement in the overall matter being investigated, interference with the privacy of such individuals should not be considered as collateral intrusion but as intended intrusion. Any such surveillance should be very carefully considered against the necessity and proportionality criteria.

'Confidential information' It should be unlikely that confidential information will be obtained during the course of an investigation undertaken by a Local Authority investigator, no matter in what capacity.

Confidential information consists of:

- Matters subject to Legal Privilege
- Confidential Personal Information
- Confidential Journalistic Material
- Parliamentary Information about Constituency Matters

This means information consisting of confidential personal information, confidential journalistic information and information relating to the spiritual, physical or mental health of an individual (whether living or dead) who can be identified from it, such as consultations between a health professional and a patient or information from a patient's medical records. It also includes confidential discussions between Members of Parliament.

In the case of local authorities, where the likely consequence of the surveillance being undertaken would be the acquisition of 'confidential information' the surveillance would require a higher level of authorisation than would normally be the case and in connection with serious crime. In this authorisation should come from the Managing Director.

Matters subject to legal privilege should not be obtained under any circumstances.

'Codes of Practice' means the Code of Practice – Covert Surveillance and Property Interference Code of Practice and the Code of Practice - Covert Human Intelligence Sources published by the Home Office

The Codes of Practice are admissible as evidence in civil and criminal proceedings and so it is essential that all officers engaged in any surveillance activity both read them and adhere to them.

***'*Communication Data'** for the purpose of this policy is any communication traffic or information sent via a telecommunication system or via the post and refers to any use of such a system by any person and available to Local Authorities when it contains the 'who', 'when' and 'where' of a communication but not the 'what' (i.e. the content of what was said or written).

'CHIS' means covert human intelligence sources as defined in Part 8 of this policy.

3.0 General Principles

3.1 As a part of the process for the investigation, prevention and enforcement of suspected criminal offences, and in connection with the prevention of disorder offences, a Local Authority is permitted to conduct observations and surveillance in pursuit of its enquiries.

3.2 However, if a Local Authority wishes to deploy **Directed Surveillance** then it can do so **only** for the purpose of preventing and detecting crime and preventing disorder and then **only** when the suspected criminal offences attracts a maximum custodial sentence of 6 months or more or is a criminal offence relating to the underage sale of tobacco or alcohol.

3.3 As stated, not all surveillance constitutes Directed Surveillance in which case there is no requirement to obtain RIPA authorisation. **Overt** surveillance is such an example, as is the deployment of covert surveillance in circumstances where there is little or no likelihood of any private information being obtained. However, this may not always be the case and in some investigations other forms of private information may be being obtained through other legal gateways – bank accounts for example.

In a case where other enquiries are being undertaken which may obtain private information be it in the private or public domains, then the holistic nature of the enquiry has to be taken into account and if private information is sought from any source, then RIPA authorisation **must** be obtained for **any** form of covert surveillance.

3.4 Local Authorities are not permitted to deploy Intrusive Surveillance but it is important to recognise that any surveillance is invasive, even if it is not intrusive as defined. Issues such as proportionality, necessity, collateral intrusion or the possibility of obtaining private information are very relevant when considering any form of surveillance. Therefore, for the purpose of any investigation or enforcement activity where **any** form of surveillance is going to be deployed, this will be subject to a considered application and authorisation process.

3.5 ‘Drive bys’ and ‘Surveillance surveys’ will not be deemed to be Directed Surveillance and will normally not require RIPA Authorisation.

3.6 For the purpose of conducting **any** surveillance, the following procedures will be followed to ensure adherence to the principles detailed in this policy. These procedures consist of two sections, the first dealing with Directed Surveillance and the second concerning General Surveillance.

3.7 Further powers to obtain telecommunications data are also conferred upon local authorities and these will be described in Section Three.

SECTION ONE - DIRECTED SURVEILLANCE AND CHIS

4.0 Preliminaries

4.1 Prior to any application being made, it will be the responsibility of the investigating officer to consider the following:

- Is the proposed surveillance **lawful** - prevention or detection of crime or prevention of disorder?
- Is surveillance **necessary** to progress the investigation?
- Is surveillance **proportionate** taking into account the seriousness of the offence?
- Is there a **less intrusive** alternative for obtaining the information?
- Why the surveillance proposed constitutes **'Directed Surveillance.'**
- Does the suspected criminal offence comply with the requirements of the Protection of Freedoms Act 2012? Does it attract a maximum custodial sentence of 6 months or more, or is the offence a criminal offence relating to the underage sale of tobacco or alcohol?

4.2 Having established that Directed Surveillance is appropriate, the investigator may conduct a 'drive by' of the location for the purpose of determining the practicality of mounting the surveillance. For this purpose, 'drive by' does not mean that the investigator cannot park or stop in order to assess the situation, but does mean that the investigator will remain in situ for only as long as is necessary for that purpose.

4.3 For the purpose of assessing the practicalities of mounting the surveillance, consideration will then be given to the following:

- Possibility of collateral intrusion;
- Distance between the observation point and the subject;
- Obstructions between the observation point and the subject;
- Visibility anticipated during the proposed periods of surveillance;
- Prospect of recognition of the subject;

- Any health and safety considerations.

4.4 Although not compulsory, it may be helpful for the investigator to draw a brief plan of the location detailing the Observation Point and area, subject to the proposed surveillance e.g. the subject's residence etc.

5.0 Application

5.1 For the purposes of any form of surveillance, be it Directed or otherwise, all applications, renewals, cancellations and RIPA data will be recorded on the appropriate documentation. These documents should be personalised for the appropriate LA/Department, although this is not compulsory. The form can be found at https://www.gov.uk/government/publications/application-for-use-of-directed-surveillance

5.2 The application form should be completed in full and should contain sufficient information to enable the person considering granting authorisation to make the decision based on the information contained therein and not with recourse to any additional material. It should contain the following:

- the reasons why the application is for Directed Surveillance;
- the reasons why the authorisation is necessary in the particular case and on the grounds (e.g. for the purpose of preventing or detecting crime/preventing disorder) listed in Section 28(3) of the 2000 Act and lawful in accordance with the requirements of the Protection of Freedoms Act 2012;
- A description of the offence and the relevant legislation sufficient to establish that the offence being investigated/prevented constitutes a serious crime;
- the nature of the surveillance;
- the identities, where known, of those to be the subject of the surveillance;
- an explanation of the information which it is desired to obtain as a result of the surveillance;
- the reasons why the surveillance is considered proportionate to what it seeks to achieve;
- details of any potential collateral intrusion and why the intrusion is justified;
- details of any confidential information that is likely to be obtained as a consequence of the surveillance;

- a subsequent record of whether authority was given or refused, by whom and the time and date.

5.3 It is essential that the extent of the covert surveillance is fully explained on the application form because the authorisation only permits the activities stated upon it. If an applicant does not include a particular activity within the authorisation form and then conducts that activity it will not be authorised and the activity will, prima facie, be unlawful and any evidence gathered may be inadmissible.

5.4 On completion of the form:

- The application form should be given directly to the applicant's Line Manager for comments and then to the Authorising Officer for consideration.

- Regardless of whether or not the application is approved, an entry should be made on the RIPA Matrix held by the Council's RIPA SPOC Officer. This document must contain details of all applications made, regardless of whether or not authorisation was granted. In addition, the matrix should also record the date of authorisation and details of the authorising officer, date of expiry of the 3 month period, dates of reviews and date of cancellation.

- The application form granted or otherwise, should be sent to the SPOC and a copy held on file in a secure location for reference by the investigation officer or any other person required so to do.

- Once an application has been authorised by the Authority it will then be subject to section 37 and 38 of the Protection of Freedoms Act 2012. This will require the Authority to obtain an order approving the granting of the authorisation, or renewal of an existing authorisation from a Justice of the Peace, be it a District Judge or lay magistrate.

- If granted, surveillance must not continue beyond the date specified in the application/renewal and cancelled appropriately or in any case after a period of 3 months less one day, whichever is the lesser, without it having been reviewed or renewed.

6.0 Authorisations

6.1 Directed Surveillance within the scope of this Policy needs to be properly authorised and recorded. An authorisation must be in writing to and authorised personally by an Authorising Officer. A list of the Authorising Officers can be found at Appendix 1 and may be revised as required. No other person may authorise applications.

6.2 It is critically important that the extent of the Directed Surveillance is fully explained on the application form because the authorisation only permits the activities stated upon it as at Para 5.4 above

6.3 The Authorising Officer must fill in the appropriate details of the authorisation upon the relevant application form and keep a copy of those documents. A copy of the forms must be forward to the SPOC.

6.4 In cases where observations are being conducted from premises with the permission of the owner consideration has to be given to the question of seeking public interest immunity to allow for the exclusion of material which identifies the location of an observation point, in order to protect the identity of owners and occupiers of the same. Watkins LJ in R. v. Johnson [1989] 1 All ER 121 at 128, Court of Appeal, gave the following ruling for a trial judge assessing such an application [editorial in bold type]:

> "The minimum evidential requirements seem to us to be the following.
> (a) The police officer in charge of the observations to be conducted, and no one of lower rank than a sergeant **[it is suggested, in the case of the Council, the Applicant]** should usually be acceptable for this purpose, must be able to testify that beforehand he visited all observation places to be used and ascertained the attitude of the occupiers of premises , not only to the use to be made of them but also to the possible disclosure thereafter of the use made and the facts which could lead to the identification of the premises thereafter and of the occupiers. He may, of course, in addition inform the court of difficulties, if any, usually encountered in the particular locality of obtaining assistance from the public.
>
> (b) A police officer of no lower rank than a chief inspector **[it is suggested, in the case of the Council, a Head of Service]** must be able to testify that immediately prior to the trial he visited the places used for observation, the results of which it is proposed to give in evidence, and ascertained whether the occupiers are the same as when the observations took place and, whether they are or are not, what the attitude of those occupiers is to the possible disclosure of the use previously made of the premises and of facts which could lead at trial to identification of premises and occupiers. Such evidence will of course be given in the absence of the jury **[and, it is argued, the defence]** when the application to exclude the material evidence is made".

It is for this reason that it is likely any documentation regarding the above will marked 'sensitive' for disclosure purposes. Further reference should be made to the Criminal Procedure and Investigations Act 1996 and to the Code of Practice issued pursuant to section 23(1) of that Act.

6.5 In general, the Authorising Officer should not be directly involved in the investigation or operation in question. Should this be unavoidable for operational reasons, this should be highlighted in the information passed to the central record of authorisations.

6.6 Authorisations will cease to have effect after three months unless renewed or cancelled on the grounds that the aims of the surveillance have been achieved or it is no longer needed. Authorisations for surveillance may stipulate that they should be reviewed after a lesser period but will always remain in effect for three months unless previously cancelled. All applications should be cancelled or renewed within 3 months less a day.

7.0 Magisterial Approval

7.1 With effect from 1 November 2012, once an application has been authorised by the Authority it will then be subject to section 37 and 38 of the Protection of Freedoms Act 2012. This will require the Authority to obtain an order approving the granting of the authorisation, or renewal of an existing authorisation from a Justice of the Peace (JP), be it a District Judge or lay magistrate.

7.2 The application to the JP must be made by the Authority which approved the application and not by a third party. The officer designated to undertake the judicial approval application must be so designated under S.223 of the Local Government Act 1972.

7.3 Following approval by an Authorising Officer, an appropriate officer, normally the officer in charge of the case, or possible the Authority's RIPA SPOC, will partially complete an application for judicial approval form, a copy of which will be attached to the file. The officer will then contact Her Majesty's Courts and Tribunal Service (HMCTS) Administration Team for a hearing date. Normally this can be arranged in 'office hours' by contacting the Listing officer at Northampton HMCTS who will make arrangements for the hearing to take place at the first available opportunity.

7.4 On the rare occasions where an urgent 'out of hours' approval is required then the officer dealing will refer to the Magistrates Clerk's 'out of hours' rota which will be held by the SPOC. This process should only be used in emergencies and should not be used simply because the application has been made late. The required hearing will then be arranged. It is highly unlikely that the 'out of hours' procedure will ever

be invoked and officers should be mindful that if they are acting in immediate response to events they do not require RIPA authorisation at that time and that the subsequent application can and should be made during normal hours should they wish to continue with the surveillance.

7.5 Once the hearing has been arranged, it is desirable that the Authorising Officer and the officer dealing will attend the court as required as it is the Authorisation which will be subject to scrutiny by the magistrate and not the investigation. He/she will be in possession of copies of the following documents which will be passed to the court clerk prior to the hearing:

- the judicial approval application form;
- the authorised RIPA application;
- any subsequent renewals/judicial notices;
- any supporting documentation.

7.6 The hearing is a 'legal proceeding' and as such the officer/s will be formally designated to appear; will required to be sworn in and to present the case for the approval of the application to the magistrate under oath; give evidence and answer any questions or queries. This process will be similar to that of a warrant application and will not be undertaken in open court. However it must be stressed that the forms and documents provided must make the case in themselves and the applicant should not rely on oral evidence presented at the hearing.

7.7. The JP will then decide whether he or she is satisfied that at the time that the authorisation was granted/renewed or a previous notice was granted/renewed that:

- the authorisation is lawful;
- there are reasonable grounds for believing that the authorisation/notice was necessary and proportionate;
- the person making the application is an appropriate designated person within the Authority who granted the authorisation and
- that the authorisation had been made in accordance with any legal restrictions e.g. that it is in connection with the prevention or detection of crime or disorder and that the suspected criminal offence attracts a maximum custodial sentence of 6 months or more, or the offence is a criminal offence relating to the underage sale of tobacco or alcohol.

7.8 The decision will be recorded on the application form and a copy will be retained by HMCTS. A copy of the decision must also be provided to

the Authority's SPOC and the original kept of the file. The decision must be complied with.

7.9 If the Authority considers that insufficient information was provided at the hearing and it is for this reason that a negative decision was made, they may consider re-applying but if the refusal was on the grounds of insufficient necessity or proportionality, or that the application contravened a legal restriction then unless there has been a significant change in the circumstances since the last application, it would be unlikely to succeed.

7.10 The application for judicial approval form can be found in the RIPA documents saved on the intranet as well as at the back of this policy which gives a process map of the authorisation application process.

7.11 Follow this link to the Protection of Freedoms Act 2012 – changes to provisions under the Regulation of Investigatory Powers Act 2000 (RIPA) guidance document produced by the

Home Office https://www.legislation.gov.uk/ukpga/2012/9/section/38

This should be read in full by all officers engaged in the process.

8.0 Covert Human Intelligence Source – (CHIS)

8.1 A person is a CHIS if:

- He/she establishes or maintains a personal or other relationship with a person for the covert purpose of:
- obtaining information or to provide access to information to another person: or
- discloses information obtained by the use of such a relationship or as a consequence of the existence of such a relationship.

8.2 A CHIS is basically an agent, informant or possibly an officer working undercover and either developing a new or maintaining an existing relationship with a subject for the purpose of covertly obtaining information – the kind of activity commonly used by the Police, Security Service, Customs & Excise, other intelligence services etc.

8.3 The provisions of RIPA are not intended to apply in circumstances where members of the public volunteer information as part of their normal civic duties, or to contact numbers set up to receive information e.g. Crime stoppers or Anti-fraud Hotline.

8.4 However, a member of the public giving information will become a CHIS if the information which he/she passes to the Council has been

covertly obtained in the course of (or as a consequence of the existence of) a personal or other relationship.

8.5 When an informant gives repeated information about a suspect or about a family, and it becomes apparent that the informant may be obtaining that information in the course of a family or neighbourhood relationship, then legal advice must be sought as it is likely that the informant may in reality be a CHIS.

8.6 KBC can lawfully use a CHIS only for the purpose of preventing or detecting crime; only in connection with a serious offence and then only when authorised by a Magistrate. However, in practice, there are insufficient resources, knowledge or experience to ensure that the Council's responsibilities can be fulfilled and so under **no** circumstances will the use of a CHIS be authorised. If any officer is in doubt about an issue which they think may constitute a CHIS they must seek legal advice.

8.7 Social Media used for surveillance purposes has the potential to become a CHIS, or even a Directed Surveillance issue. As the result of the proliferation in the use of social media such as Facebook, Twitter and others, even E bay, a considered approach is required to establish whether or not the use of the technique constitutes either Directed Surveillance or a CHIS when using these as sources of information in pursuit of an investigation.

8.8 If an individual places material in the public domain and does not apply any privacy controls to it, then this, if used alone, has to be considered open source for the purposes of using that material in connection with an investigation. However, the same would not apply if the investigator were to subvert any privacy settings by becoming a 'friend' for the purposes of e.g. Facebook and if he were to then covertly exploit that relationship to obtain material for use in that investigation. Then a CHIS issue would apply and the investigator would be in breach RIPA and the Council's policy.

8.9 Furthermore, repeated or systematic visits to any open source site would in all likelihood be conducted covertly, and could constitute Directed Surveillance with a requirement that the appropriate authorisation should be obtained considered. Moreover, information obtained from such means if used with other information obtained elsewhere with a view to building up a profile of the subject, then the totality of the information obtained could be construed as 'private' with all the applicable RIPA ramifications. Again, when in doubt, any officer should seek legal opinion.

8.10 In the case of any Social Networking sites, such as E bay for example, merely examining public feedback to gauge the level and type of sales listed would not in itself constitute DS or CHIS, and neither would a one

off test purchase.

9.0 Surveillance Activity

9.1 The purpose of this document is to identify the correct procedures for applying and monitoring RIPA applications and is not intended to detail how the surveillance will be undertaken as this will be largely determined by the circumstances of the individual investigation.

9.2 However, all surveillance must be undertaken in accordance with legislative requirements and rules of evidence and it would be suggested that prior to commencing any surveillance, the officers concerned should have completed appropriate training. Most importantly, the surveillance must be carried out in accordance with that authorised on the application and should not extend beyond the bounds of that authorisation without having been reviewed and approved beforehand.

10.0 Reviews/Renewals

10.1 Reviews - An internal review of the surveillance should be carried out on a regular basis. Is an internal function and should not be confused with a renewal which requires magisterial authorisation. An internal review may be considered an appropriate measure to determine if the surveillance should be cancelled before the expiry of the authorisation, or to continue beyond a pre-determined period, this being less than the statutory 3 months authorisation. The form can be fund at https://www.gov.uk/government/publications/renewal-form-for-directed-surveillance

10.2 Renewal - In the case where it is considered that the surveillance carried out within the 3 month authorisation period was insufficient to achieve the desired outcome, or that the activity applied for was inadequate to achieve the desired objective, and there are grounds to consider that a continuance/extension of and or change to the surveillance previously authorised, may result further information being obtained, the following will apply:

- A renewal form should be submitted outlining the reasons for the application. The form can be found at can be found at https://www.gov.uk/government/publications/renewal-form-for-directed-surveillance .

- The application form should be given directly to the applicant's Line Manager for comments and then to the authorising officer for consideration, if they are not one and the same.

- An entry should be made on the RIPA Matrix, against the appropriate application. This document must contain details of all applications made, as well as details of the authorising officer, date

of expiry of the 3 month period, dates of reviews and date of cancellation.

- The renewal, granted or otherwise, should be sent to the Authorising Officer and a copy held on file in a secure location for reference by the investigation officer or any other person required so to do.

- If granted, surveillance must not continue beyond the date specified in the renewal or for a period in excess of 3 months, whichever is the lesser, without having been further reviewed and renewed.

- Refer to para 7.5 – any renewal will be subject to Magisterial Consideration following the process outlined.

11.0 Cancellations

11.1 Surveillance will be terminated immediately when:

- It is considered that the surveillance has achieved the desired result, and sufficient evidence has been obtained to substantiate the allegation;

- or that there is sufficient evidence to disprove the allegation;

- or there are no grounds to consider that a continuance of the surveillance may result in the desired information being obtained;

- or where the period granted for the surveillance or 3 months have expired, whichever is the lesser, the surveillance will be cancelled.

11.2 To cancel surveillance a cancellation form will be submitted. A copy of the form can be found at https://www.gov.uk/government/publications/cancellation-of-use-of-directed-surveillance-form and the following process will apply:

- the cancellation form should be given directly to the applicant's Line Manager for comment and then to the Authorising Officer for approval.

- An entry should be made on the RIPA Matrix, against the appropriate application. This document must contain details of all applications made, as well as details of the Authorising Officer, date of expiry of the 3 month period, dates of reviews and date of cancellation.

- The cancellation should be sent to the Authorising Officer and a copy held on file in a secure location for reference by the investigation officer or any other person required so to do.

- The cancellation should be completed and processed immediately at the end of the period specified in the application or renewal or within a period of 3 months, whichever is the lesser.

- In order to comply with data protection legislation, at the termination of the activity, unless any evidence of criminal or anti social behaviour is recorded and is to be used in connection with any further investigation, including one which may involve the future deployment of Directed Surveillance, the evidence gathered as a result of the covert surveillance will be destroyed and a note made to this effect on the Directed Surveillance Cancellation form.

12.0 Immediate Response

12.1 In a case where an officer is acting in immediate response to events or circumstances it is permissible to conduct surveillance without having obtained written or magisterial authorisation. If this is the case the following will apply:

- At the first opportunity, the appropriate application form must be completed.

- The application form should be given directly to the applicant's line manager for comments and then to the authorising officer for consideration, if they are not one and the same.

- An entry should be made on the RIPA Matrix and the application sent to the Authority's SPOC and a copy held in a secure location for reference by the investigation officer or any other person required so to do.

- Refer to para 7.5 – any subsequent application will be subject to Magisterial Consideration following the process outlined.

13.0 Joint Investigations

13.1 In many cases, investigations are conducted in conjunction with other benefit agencies such as the DWP, HMRC, Trading Standards and the Police etc. It is usual practice that one of the participants is designated as the lead agency and so would assume the responsibility of undertaking certain functions, surveillance applications being one of them.

13.2 It is unreasonable to expect all of the participating agencies to apply and monitor the surveillance being conducted on one specific operation, so in the case of joint agency working, the following will apply:

- One of the participating agencies to be designated as the lead – this normally defaults to the agency which instigated the investigation. Agreement to be noted on the application form

- The application form should be given directly to the applicant's Line Manager for comments and then to the authorising officer for consideration, if they are not one and the same.

- A copy of the completed application form should be forwarded to the investigation officer from each other participating agency for their attention.

- Refer to para 7.5 – any application made by a local Authority will be subject to Magisterial Consideration following the process outlined. In the case of other agencies, this requirement may not apply.

14.0 Records

14.1 All records maintained under the Act must be kept secure and confidential. A central record of all authorisations, reviews, renewals, cancellations and refusals, whatever the type of surveillance, is held by the SPOC –RIPA Coordinator. Copies of all such papers must be forwarded to that officer at the earliest opportunity either by providing hard copies or scanning and providing electronic copies. If hard copies are sent an advisory e-mail should be sent when they are sent as a check in case they go missing. Documents should be sent in sealed envelopes and marked 'Strictly Private & Confidential' or delivered by hand. If being provided electronically, the original signed forms should be scanned and they should be encrypted if appropriate.

SECTION TWO - GENERAL SURVEILLANCE

15.0 Preliminaries

15.1 There may be occasions where **overt** surveillance or some other form of surveillance which does not require RIPA authorisation is under consideration e.g. where there is **no** prospect of obtaining any private information about anyone.

15.2 In fact every effort should be taken to obtain evidence sufficient to prove the offence without the need to deploy surveillance and it is recognised advice that Directed Surveillance should be used as a **'last resort.'** In all cases if there are less intrusive means of obtaining the required information then these should be deployed in preference to deploying Directed Surveillance or indeed, any form of surveillance. This could include amongst other things, witness evidence, documentary evidence and even interviewing the suspected offender if there is one. Even if some form of surveillance is deemed necessary 'overt' surveillance may suffice in which case magisterial approval is not required.

15.3 This principle is not unlike the concept of 'tax avoidance' and 'tax evasion'. It may be perfectly possible to 'avoid' the need for RIPA authorisation by not deploying surveillance but by obtaining the evidence by less intrusive means, or if some form of surveillance is required, ensuring it is **overt.** However, where there is a **need** for the deployment of Directed Surveillance, it is **essential** that the application and authorisation process authorisation is not 'evaded' and that the appropriate forms are completed, submitted, approved and magisterial consent is obtained before the activity takes place.

15.4 Even the concept of what is considered to be **'overt'** should be seriously considered – something that may, on the face of it appear to be overt may not in fact be so – would a local government officer undertaking benefit fraud surveillance be acting overtly merely by conducting the surveillance from a marked council vehicle – probably this would be covert – whereas another local authority officer employed as a dog warden who is conducting surveillance to catch a 'serial dog fowler', when conducting the surveillance from clearly marked 'dog warden van' may well be overt. It is a requirement that the Authority takes all practical steps to ensure that the overt activity is exactly that, either by clear and adequate signage that an area is under surveillance or by notifying anyone who could be affected by the activity being deployed.

15.5 However, in the case where static cameras are deployed as a preventative measure, to ensure that the activity is overt and in order to make it clear to anyone in the vicinity of the cameras that the area is under surveillance, clear signage will be displayed and the signs will be clearly marked with the KBC logo.

15.6 In cases where General Surveillance is deployed, although RIPA authorisation is not required, there should be some consideration of the factors which could be of concern to anyone subject to the surveillance, third parties or any other interested party and the Authorising Officer should make a record of their decisions.

15.7 As in the case of RIPA applications the points to consider are outlined at paras 2.1.to 2.4 and a drive by and sketch plan may be considered as part of the assessment process. It is essential that the sketch plan includes the locations of the signs and field of view covered by the cameras.

16.0 Application

16.1 All applications, renewals, cancellations for general surveillance should be documented by the Authorising Officer.

16.2 The application form should be completed in full and should contain sufficient information to enable the person considering granting authorisation to make the decision based on the information contained therein and not with recourse to any additional material.

16.3 On completion, the application form should be given directly to the applicant's Line Manager for comments and then to the authorising officer for consideration, if they are not one and the same. Details of the application do not have to be entered on the RIPA matrix.

16.4 So as to eliminate any doubt, the Authorising Officer should stipulate fully what activity is being authorised, even if this is a direct repetition of the activity being applied for.

17.0 Surveillance Activity

17.1 As in the case of RIPA, this procedure does not attempt to deal with surveillance techniques, although, in this case, the officer must ensure that a RIPA authorisation is 'not' required for the appropriate reasons, which will usually be one or more of the following:

- Primarily, the surveillance is overt, ensuring that everyone subject to the surveillance is aware that it is taking place.

- There is little or no likelihood that private information about anyone will be obtained – the information to be obtained merely relates to the commission of an offence such as painting graffiti or the level of noise being generated as opposed to the actual content of the noise and the issues surrounding collateral intrusion have been resolved.

- The surveillance is in immediate response to events although, as in the case of Directed Surveillance, it may be impractical to complete

the required paperwork there and then but as soon as practicable afterwards.

- The surveillance is not directed against a person/people but against an inanimate object such as the mere presence of vehicle or in relation to offences taking place on land where there is no specific suspect.

17.2 Again, all surveillance must be undertaken in accordance with legislative requirements and rules of evidence and it would be suggested that prior to commencing any surveillance, the officers concerned should have completed appropriate training.

18.0 Cancellations

18.1 Surveillance will be terminated immediately, and notification provided on the relevant form, when it is deemed to be no longer required.

18.2 The cancellation form should be given directly to the applicant's Line Manager for comment and then to the authorising officer for countersignature, if they are not one and the same. After being signed they should be retained on the investigation file.

18.3 In order to comply with data protection legislation, at the termination of the activity, unless any evidence of criminal or anti social behaviour is recorded and to be used in connection with any further investigation, including one which may involve the future deployment of Directed Surveillance, the evidence gathered as a result of the overt surveillance will be destroyed and a note made to this effect on the Surveillance Cancellation form.

19.0 Confidential Information

19.1 There is no possibility that the acquisition of Confidential Information (as defined in para 2) can be authorised as a result of General Observations in any circumstances as the very nature of the material obtained is to be considered 'private' and therefore a RIPA authorisation, approved by the Chief Executive will be required.

20.0 Conclusion

20.1 RIPA does not deal with the material or information obtained as a result of surveillance. The managing and handling of such material of information must be strictly in accordance with the Data Protection Act, 1998 and the Criminal Procedure and Investigations Act, 1996. Officers should ensure that any material is managed and handled properly and in accordance with these provisions and any other statutory or other requirements that may apply from time to time. Failure to do so may render the material or information inadmissible as well as exposing the Council to risk.

20.2 However, if this policy and procedures are adhered to, then the element of risk connected to the Council's deployment of Directed or General Surveillance will be substantially mitigated against.

SECTION THREE – COMMUNICATIONS DATA

21.1 Introduction

21.2 We live in an increasingly communication based society and many forms of unlawful or antisocial behaviour manifest themselves via telecommunications e.g. 'trolling.' Very often there can be a communication trail which provides evidence to support an investigation.

21.3 The acquisition of communication data is available to Local Authorities under certain circumstances - for the prevention and detection of crime or preventing disorder (Section 22(2)(b) of RIPA). However, unlike Directed Surveillance, there is no sentencing condition to consider before making an application.

21.4 In summary - Communications Data (CD) available to Local Authorities contains the 'who', 'when' and 'where' of a communication but not the 'what' (i.e. the content of what was said or written).

22.1 Communication data

22.2 Communication data for the purpose of this policy is any communication traffic or information sent via a telecommunication system or via the post and refers to any use of such a system by any person.

22.3 RIPA breaks this definition down into three categories, each covered by separate sections of the Act Section 21(4)(a) – Information regarding communications data/traffic:

- Traffic data obtained and held by the communications service provider regarding the account holders use of the service – the things that make the communication work or where information may be stored.

- Local authorities do **not** have access to this information.

Section 21(4)(b) – Information regarding use of services:

- 'Everyday information' about times/dates calls were made, duration of such calls, and the numbers called or received, sent e mail logs (not the content of), service connection, conference calling logs and call barring, forwarding and re-direction details and details of recordable post.

- Local authorities can access this information.

Section 21(4)(c) - Information about service users

- Subscriber account details, names and addresses, installation and billing addresses, payment and contact details.

- Local authorities can access this information.

23.1 General Principles

23.2 Local authorities can obtain information about service users and the use of services and there are occasions where this could be useful such as a serious Anti-Social Behaviour case where harassment is taking place via a mobile phone and correlating the time of calls made to a particular number with information provided by the complainant may support or further the investigation.

23.3 But the same rules for applying and authorising this activity apply - necessity, proportionality etc. – these will have to be followed as they would for Directed or General Surveillance.

24.1 How we obtain the Information

24.2 Under RIPA Section 22(3) you could request to be authorised to obtain this information yourself, extracting the data directly from the Communication Service Provider's (CSP) records. More likely you are going to utilise RIPA Section 22(4) and request the communication service from an authorised provider and in practice this will be via the National Anti-Fraud Network which for the purposes of these applications will act as the SPOC for the Authority.

24.3 The idea of only having one point of contact for each public authority was agreed between the Home Office and the Communication Service Provider's to ensure data was only supplied to those entitled to obtain the data. Only the SPOC(NAFN) can acquire communications data on behalf of the Council.

24.4 The investigating officer must complete an application form in full with no sections omitted.
(https://www.gov.uk/government/publications/chapter-ii-application-for-communications-data)
The form is subject to inspection by the Interception of Communications Commissioner and the applicant may be asked to justify their application.

24.5 The SPOC will then assess whether the form is completed properly, that the request is lawful, the request is one to which the CSP can practically respond and that the cost and resource implications for the CSP/Council are within reason after which the SPOC will then submit the form to the Authorising Officer for authorisation.

24.6 The application must then be approved by a Magistrate. The investigating officer should liaise with the Authority's Legal Department

to obtain this authorisation after which a hearing will be arranged with the Court to seek the Magistrate's approval. See Section One Para 7.3

.

24.7 Once authorised, the SPOC will forward the application to the CSP and once the data sought is returned to the SPOC, a copy of the information will be passed to the applicant.

24.8 Authorisations to collect communications data under s22(3) have a life span of one month. However, they can be renewed by serving a new authorisation or notice for further months, within any time within the current life of the notice. Magistrates would need to approve any renewal.

APPENDIX 1

REGULATION OF INVESTIGATORY POWERS ACT 2000

Authorising Officers:

Confidential Information	Managing Director
Directed Surveillance	Managing Director
SPOC (RIPA co-ordinator)	Head of Democratic and Legal Services
All other matters	
Benefit Fraud	Head of Income and Debt Recovery
Audit Investigations	Head of Finance and Strategic Development
Planning, Listed Building & Conservation	Head of Development Services
Environmental Health	Head of Environmental Health
Housing	Head of Housing