Hinckley & Bosworth Borough Council

Hinckley & Bosworth Borough Council

Regulatory Investigatory Powers Act (RIPA) Policy

2018

Contents

A. Introduction and key contacts

Our RIPA 2018 policy is based upon the requirements of the Regulation and Investigatory Powers Act 200 ('RIPA') and the Home Office's Codes of Practices on Surveillance which support RIPA.

It also reflects the recommendations arising from the last RIPA inspection carried out in 2017.

The authoritative position on RIPA is the Act itself and any officer who is unsure about any aspect of this document should contact, at the earliest possible opportunity, the Information Governance Officer for advice and assistance. A copy of this document is on the intranet and is reviewed annually.

The purpose of RIPA is to regulate the "interception of communications, the acquisition and disclosure of data relating to communications, the carrying out of surveillance, the use of covert human intelligence sources and the acquisition of the means by which electronic data protected by encryption or passwords may be decrypted or accessed."

The purpose of this policy document is to ensure that any investigation thought necessary by the council involving directed surveillance, Covert Human Intelligence Sources (CHIS) or the acquisition of data, is carried out effectively, respecting human rights and in accordance with the law.

Senior Responsible Officer (SRO)

Julie Kenny, Director of Corporate Services, is the council's Senior Responsible Officer for RIPA. The SRO is responsible for:

- Specifying, by name, appropriate officers able to grant RIPA authorisations (Authorising officers)
- Verifying the competency of those officers before authorising them
- Ensuring the integrity of the surveillance processes in place and compliance with legislation and Office Codes of Practice
- Engagement with Surveillance Commissioner and inspector when they conduct their inspections
- Overseeing implementation of any post inspection action plans.

Information Governance Officer

For all legal advice, please refer to the SRO or the Information Governance Officer.

The Information Governance Officer is responsible for maintaining the central register of all RIPA authorisations, reviews, renewals, cancellations and rejections.

It is the responsibility of the relevant Authorising Officer, however, to ensure that the original forms are sent to the Senior Responsible Officer, Authorising officers must also ensure that, when sending the completed forms, they are sent in a confidential manner.

RIPA and this document are important for the effective and efficient operations of the Borough Council's actions with regard to covert surveillance and Covert Human Intelligence Sources (CHIS).

This document will, therefore, be kept under annual review by the Information Governance Officer. Any officer wishing to undertake investigations under RIPA should, in the first instance, discuss matters with the Legal Services Manager and the Information Governance Officer. Further information can be found in the Office of Surveillance Commissions 'Procedures and Guidance 2016'.

Oversight

Independent oversight of the use of the powers contained within RIPA is provided by the Investigatory Powers Commissioner's Officer (IPCO). This oversight includes inspections carried out by IPCO officers.

Email monitoring

In terms of monitoring emails and internet usage, it is important to recognise the important interplay and overlaps with the council's email and internet policies and guidance, and legislation such as RIPA, subsequent statutory instruments relating to RIPA, the Data Protection Act 1998, Human Rights Act 1988. RIPA forms should be used, where relevant, and they will be only relevant where the criteria listed on the forms are fully met.

B. Background to the relevant Acts

The Human Rights Act 2000

Under legislation, it is the responsibility of all public bodes to comply fully with the requirements of the Human Rights Act (HRA) 1998, which came into force on 2 October 2000, in particular, Article 8 'the right to respect for private an family life, home and correspondence'. The Regulation of Investigatory Powers Act (RIPA) 2000 was enacted in order to give a clear statutory framework for the operation of certain intrusive investigative techniques, to provide for compliance with the HRA. RIPA also provided for the appointment of Independent Surveillance Commissioners to oversee the exercise by public authorities and duties under the Act.

Essentially, RIPA required the following human rights principles to be complied with for investigatory work:

- The proposed action must be lawful
- The proposed action must be proportionate
- The proposed action must be necessary
- The proposed action must be non-discriminatory

The Data Protection Act 2018 and the General Data Protection Regulations (GDPR)

The GDPR sets out seven key principles which must be observed when processing data:

- Lawfulness, fairness and transparency
- Purpose limitation
- Data minimisation
- Accuracy
- Storage limitation
- Integrity and confidentiality (security)
- Accountability

Officers and others using this policy and the powers under RIPA must ensure that the use and storage of any personal information obtained by these methods must be undertaken in

accordance with the Data Protection Act 2018 and the GDPR. Officers must also take account of the impact of the Freedom of Information Act 2000 and the Environmental Information Regulations 2004 in respect of any records kept as a result of investigations.

Codes of Practice

To coincide with the RIPA coming into force, the Home Officer published four statutory codes of practice, which are mandatory under the terms of the Act (Part IV, para 75(1), covering:

- Use of covert surveillance
- Use of covert human intelligence sources
- Interception of communications and accessing communications data
- Investigation of electronic data protected by encryption

The Regulation of Investigatory Powers Act states that all public authorities (including local authorities) are expected to comply with the codes.

The code of practice which has the most significant impact on the activities of officers at Hinckley & Bosworth Borough Council is the Code of Practice on Covert Surveillance. However, officers should also be aware of the Regulation of Investigatory Powers (Communications Data) order which provides guidance on the acquisition and disclosure of communications data.

C. What RIPA does and does not do

RIPA does:

- Require prior authorisation of directed surveillance
- Prohibit the council from carrying out intrusive surveillance
- Require authorisation of the conduct and use of a CHIS
- Require safeguards for the conduct and use of a CHIS
- Require judicial approval of authorisations before directed surveillance and use of CHIS can be carried out (see section J)

RIPA does not:

- Prejudice or dis-apply any existing powers available to the council to obtain information

by any means not involving conduct that may be authorised under this Act. For examples, it does not affect the council's current powers to obtain information via the DVLA, or to get information from the Land Registry as to the ownership of a property

If the Authorising Officer or any applicant is in any doubt, he/she should asked the SRP **before** any directed surveillance and/or CHIS is authorise, renewed, cancelled or rejected.

D. Types of surveillance

All authorisations, even if urgent, must be made in writing.

Surveillance is defined as including:

- Monitoring, observing, listening to persons, their movements, their conversations or their other activities
- Recording anything monitored, observed or listened to in the course of surveillance
- Surveillance by or with the assistance of a surveillance device

There are different types of surveillance:

- General surveillance (not directed at an individual)
- Covert surveillance (directed/intrusive)

RIPA authorisation is not required for all surveillance. It only applies to covert surveillance.

1. Overt surveillance

1.1 Most of the surveillance carried out by this council will be done overtly - there will be nothing secretive or hidden about it. In many cases, officers will behaving in the same way as a normal member of the public and/or will be going about council business openly (Clean Neighbourhood Officer on patrol).

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

2. Covert surveillance

2.1 In terms of RIPA, an action is defined as covert 'if, and only if, it is carry out in a manner that is calculated to ensure that the persons who are subject to surveillance are unaware that it is, or may be taking place'.

2.2 RIPA regulates two types of covert surveillance - Directed Surveillance and Intrusive Surveillance and the use of Covert Human Intelligence Sources (CHIS).

3. Directed surveillance

3.1 Surveillance is directed if it is undertaken:

- For the purpose of a specific investigation or specific operation in such a manner as is likely to result in the obtaining of private information about a person (whether or not that person is specifically targeted for purposes of an investigation)
- Is covert
- Is not intrusive surveillance (see definition below - the council must not carry out any intrusive surveillance)
- Is not carried out in an immediate response to events which would otherwise make seeking authorisation under the Act unreasonable, for example, spotting something suspicious and continue to observe it
- Since 2012, the crime suspected must pass the threshold of attracting a minimum sentence of six months imprisonment

3.2 The key issue in directed surveillance is the targeting of an individual with the intention of gaining private information. This includes any information relating to private and family life, home and correspondence. The fact that covert surveillance occurs in a public place or on business premises does not mean that it cannot result in the obtaining of private information about a person. Prolonged surveillance targeted on a single person will undoubtedly result in the obtaining of private information about him/her and others that she/he comes into contact, or associates, with.

3.3 Similarly, although overt town centre CCTV cameras do not normally require authorisation, if the camera is tasked for a specific purpose which involves prolonged surveillance on a particular person, authorisation will be required. The way a person

runs his/her business may also reveal information about his or her private life and the private life of others.

3.4 Examples of **directed** surveillance:

- **The covert taping of nuisance tenants within a neighbouring property.**
- **The use of noise nuisance recorders**
  The use of electronic noise monitoring equipment for measuring levels and frequency of noise in a complainants premises has been expressly judged by the Chief Surveillance Commissioner as not surveillance because the noise has been inflicted by the perpetrator, and thereby forfeited any claim of private, unless sensitive equipment is used to discern speech or other noisy activity not discernible by the unaided ear (Oversight arrangements for covert surveillance and property interference conducted by public authorities Office of Surveillance Commissioners, December 2011).
- The use of a town centre CCTV to track an individual in a planned operation that the individual is unaware of
- The covert observations of an individual at home but not 'intrusive'. Could include observations of a drive (fixing/washing the car)
- The covert monitoring of an individual to and from work and home
- Seeking assistance from members of the public, for example, asking them to record their neighbours and passing on the tape

3.5 Examples of **not directed** surveillance:

- Hot spot targeting. For example, Licensing Officers standing on a street to monitor private hire cars plying for hire illegally
- CCTV
- Incidental surveillance - things observed as part of the course of other duties

4. Intrusive Surveillance

4.1 Surveillance is intrusive if it:

- Is covert
- Is carried out in relation to anything taking place on any residential premises, or in any vehicle (or on certain premises

where legal consultations with professional legal advisors are taking place)

- involves the presence of an individual in the premises or in the vehicle
- Is carried out by a surveillance device in the premises/vehicle cameras, tape recorders.

4.2 However, surveillance carried out in relation to residential premises by use of a device (for example, a camera) which is not in or on the premises is not intrusive (although it will be directed), unless it is of the same quality of information as would be obtained if the equipment was in the premises/vehicle.

Intrusive surveillance can be carried out only by the Police and other law enforcement agencies. Council offices must not carry out intrusive surveillance.

Codes of practice for covert surveillance/use of a CHIS

1. The use of directed surveillance or covert human intelligence sources (CHIS) for a particular investigation must be subject to prior authorisation by an officer of a rank or position at least as senior as is specified in regulations made under RIPA.

2. The use of directed surveillance should only be authorised if the authorising officer is satisfied that the action is necessary (in a democratic society) for the prevention or detection of crime failing within the following description:
    - Crime punishable, whether on summary conviction or on indictment, by a maximum term of at least six months imprisonment
    - Crime constituting an offence under sections 146, 147, 147A of the Licensing Act, or section 7 of the Children and Young Persons Act 1933.

3. The use of covert intelligence sources should only be authorised if the authorising officer is satisfied that the action is necessary for the prevention or detection of crime and disorder.

4. If either type of surveillance is considered necessary, then the authorising officer must also be satisfied that the surveillance is proportionate - the HAR defines a measure or action as proportionate if it:
    - Impairs as little as possible the rights and freedoms (of the individual concerned and of innocent third parties)
    - Is carefully designed to meet the objectives in question
    - Is not arbitrary, unfair or based on irrational consideration

5. Essentially, the person granting the authorisation must believe that the use of a source is proportionate to what is sought to be achieved by the conduct and use of that source. This involves balancing the intrusiveness of the use of the source on the target and others who might be affected by it against the need for the source to be used in operational terms. The use of a source will not be proportionate if it is excessive and the circumstances of the case or if the information which is sought could reasonable be obtained by other less intrusive means.

    A potential model answer would make it clear that the four elements of proportionality had been fully considered:
    - Balancing the size a scope of the operation against the gravity and extent of the perceived mischief
    - Explaining how and why the methods to be adopted will cause the least possible intrusion on the target and others
    - That the activity is an appropriate use of the legislation and the only reasonable way, having considered all other, of obtaining the necessary result
    - Evidencing what other methods had been considered and why they were not implemented

6. Any surveillance involved in a case, even if it does not form part of an eventual prosecution case, may be deemed unlawful if not properly authorised and could lead to a challenge under Article 8 of the ECHR.

7. The requirements of the RIPA and the HRA impact on all officers of the council who undertake investigatory or enforcement activities, including Benefits fraud investigation, Environmental Health, Planning. The council adopts Codes of Practice which are mandatory under the Act and following procedures should be adhered to in the conduct of any covert surveillance.

Procedures for conduct of/authorisation of surveillance

A simplified way of remembering RIPA is the acronym 'PLAN' covert surveillance must be proportional, lawful, authorised and necessary:

- **P**roportional
- **L**awful (in accordance with legislation and the legality of the audit activity)
- **A**uthorised (by a proper person)
- **N**ecessary (having considered alternatives)

For any covert surveillance to be lawful, records must be sufficient to prove that RIPA has been complied with. All procedures relating to covert surveillance must be documented on standard forms. These are available from the Information Governance Officer.

Covert surveillance carried out by an officer of the council should be subject to prior authorisation by a senior officer within the council. It should not be authorised by an officer directly involved in the surveillance, so that there is independent review of whether the surveillance is necessary and proportionate. Officers designated to authorise surveillance are detailed in section H (page 16).

Application for authorisation must be made in writing and these should include full details of the proposed surveillance and the duration. The application must include full details of:

- The grounds on which the action is necessary
- Why the action is proportional to what it seeks to achieve (there must be a clear indication of what alternative methods were considered for obtaining the information required and why these were rejected). It may be useful to state that this is the only way the evidence can be gathered
- The person(s) to be subject to the action
- The action to be authorised (for example, observations/following and reference to any premises/vehicles involved and whether private/public, residential business)'
- Full description of the work to be carried out (including locations of areas from which observations are to be conducted, for example, street names and whether photography Equipment or binoculars are to be used)
- An account of the investigation/operation

- The information which is sought from the action
- The potential for collateral intrusion and a plan to minimise this potential
- The likelihood of acquiring any confidential/religious material (medical records, financial records, legal documents)

Confidential material

A higher level of authorisation is required in respect of confidential material.

In all such cases, authorisation should be obtained from the Chief Executive (or the person acting as in their absence). Confidential information consists of communications subject to legal privilege, communications between a Member of Parliament and another person on constituency matters, confidential personal information, or confidential journalistic material.

Reactive

Where surveillance is reactive (for example, an immediate response to an immediate situation), this must be documented within reasonable time of the surveillance - this time limit is three days. The authorising officer must consider whether the proposed surveillance is proportionate, lawful, necessary and non-discriminatory. If the proposed surveillance cannot be managed within the criteria, it should not be undertaken.

Is it proportional?

Surveillance activity must be proportionate to the offence under investigation.

For example, suspected theft from the workplace may merit surveillance work but not at the person's home. The length of the investigation also needs to be proportionate.

In assessing whether or not the proposed surveillance is proportionate, consideration should be given to other appropriate means of gathering the information. The least intrusive method will be considered proportionate by the courts.

Is it intrusive?

Account must be taken of the risk of intrusion into the privacy of persons other than the specified subject of the surveillance (Collateral Intrusion). Measures must be taken, wherever practicable, to avoid or minimise the collateral intrusion and the matter may be an aspect of determining proportionality.

The appropriate course of action must then be decided in terms of the type of surveillance and hence, the appropriate form/course of activity:

- Directed surveillance
- Intrusive surveillance - not be undertaken by local authority
- Use of a Covert Human Intelligence source

Intrusive surveillance is only allowed for 'serious' crimes. The police can only obtain authorisation for intrusive surveillance from the Surveillance Commissioners. Local authorities cannot undertake intrusive surveillance.

There must be appropriate arrangements in place for the management and oversight of the CHIS and this must address health and safety issues through a risk assessment.

RIPA log and register

Any surveillance should have a dedicated log-sheet for officers' use. The log-sheet should be kept in chronological order detailing who is on the surveillance, where it is and what happens. Where notes cannot be written up at the time of surveillance, it should be completed as soon as possible afterwards.

All alterations on the log-sheet should be crossed through and initialed and then the corrected material written to the side in the normal manner. Correction fluid should not be used at any time. Completion of the log-sheet should ensure that no empty lines are left where additional information could be written in at a later date. These logs-sheets could be used in the event of criminal prosecution and should be kept correctly, signed as true statements, and secure at all times.

In all cases, there is a duty of care to those surveyed. All details and approvals must be kept strictly confidential. The privacy of individuals must not be put at risk and unnecessary information should not be documented, for example, if the observed person was incidentally observed in a private context such as an extra marital affair.

Where photographs or videos are taken, then a photographic log needs to be maintained and all

negatives retained. Technology is available to alter photographs and the log-sheets are important to prove the originality of the photographs/videos.

Log-sheets should be kept locked with the rest of the supporting documents for a period of six years from the date of the court order.

All authorisations should be held at a central point with the Information Governance officer to facilitate independent examination by the Surveillance Commissioners. Copies of all authorisations and cancellations should, therefore, be forwarded to the SRO/Information Governance Officer.

A review date should be set for the authorisation and be reviewed no later than that date.

With regard to the duration of the authorisation, cancellation must be a positive act for which diary dates are set. Time limits should be placed on any authorisation for surveillance. In all cases, written 'Authorities' for directed surveillance last for three months (Authorisations for use of CHIS last for 12 months, unless relating to use of juveniles). Authorisations must then be renewed if that is deemed necessary, provided they meet the requirement for authorisation. Authorisations can be reviewed at any time and should be cancelled as soon as they are considered to be no longer necessary or appropriate. Forms are available for the cancellation and the renewal of surveillance as required.

Authorisations last for:

- 72 hours if not renewed.
- If it is non-urgent and is in writing, three months for directed surveillance.

The power to make urgent oral authorisations has been removed because section 43(1) (a) of RIPA no longer applies to authorisations requiring a magistrate's approvals. **All authorisations, even if urgent, must be made in writing.**

Officers permitted to authorise a covert surveillance exercise -

Authorising Officers

Directed surveillance and the use of a CHIS can only be lawfully carried out if properly authorised, and in strict accordance with the terms of the authorisation.

The Senior Responsible Officer will ensure that sufficient numbers of Authorising Officers from each service are, after suitable training on RIPA and this document, duly certified to take action under this document.

It will be the responsibility of Authorising Officers who have been duly certified, to ensure their relevant members of staff are also suitably trained as 'applicants' so as to avoid common mistakes appearing on forms for RIPA authorisations.

Authorising Officers must also pay particular attention to Health and Safety issues that may be raised by any proposed surveillance activity. Under no circumstances, should an Authorising Officer approve any RIPA form unless, and until s/he is satisfied the health and safety of the council employees/agents are suitably addressed and/or risks minimised, so far as is possible, and proportionate to/with the surveillance being proposed. If an Authorising Officer is in any doubt, s/he should obtain prior guidance on the same from the SRO.

The officers permitted to authorise a covert surveillance exercise at the council (Authorising Officers) are:

- Julie Kenny, Director of Corporate Services
- Bill Cullen, Chief Executive
- Sharon Stacey, Director of Community Services

Prior to operating their powers to authorise surveillance, such officers must have undertaken such training as deemed appropriate by the SRO. A record of officers who have undertaken training will be kept by the SRO.

To authorise directed surveillance, the Authorising Officer must demonstrate that the proposed activity is necessary for the prevention or detection of a crime which either carries a maximum sentence of at least six months' imprisonment, or is an offence relating to the sale of alcohol or tobacco products to minors. (As to the definition of 'detecting crime', see RIPA section 81(5).

Absence of Authorising Officer (section 94(1) of PA97, section 34(2) of RIPA and section 12(2) of RIP(S)A)

It is unlikely to be regarded as 'not reasonably practicable' (within the meaning of sections of the Acts specified above) for an Authorising Officer to consider an application, unless he/she is too ill to give attention, on annual leave, is absent from his/her office and his/her home, or is for some reason not able, within a reasonable time, to obtain access to a secure telephone or fax machine. Pressure of work is not to be regarded as rendering it impracticable for an Authorising Officer to consider an application. Where a deputy acts in their stead, this should be on a substantive officer basis and not a temporary or convenient arrangement to the Authorising Officer.

Where a designated deputy gives an authorising, the reason for the absence of the Authorising Officer should be stated.

Acquisition and disclosure of communications data

1. Communications data is information held by communication service providers (telecom, internet and postal companies). The Act makes provision for obtaining communications data from such service providers and the disclosure of any person of such data. Communications data includes information relating to the use of a postal service or telecommunicationsystem but does not include the contents of the communication itself.

2. Examples of 'data' available to the council under the Act include:
    - Postal item (anything written on the outside of the envelope)
    - Telephone (personal details of the subscriber, the telephone number and itemised calls made)
    - E-mail and internet (details of the subscriber of e-mail account, websites visited, details and date and time e-mails sent and received)

3. Communications data can only be obtained for the sole purpose of the prevention/detection of crime and/or disorder. Further test of necessity must be met before data is obtained. The Authorising Officer must also consider the conduct involved in obtaining the communications data to be proportionate to what it is sought to achieve and must also consider the risk of collateral intrusion.

4. Communications data can be accessed using two different methods:
    - The granting or authorisations
    - The service of notices.

5. An authorisation would allow the council to collect or retrieve the data itself from the service provider. A notice is given by the council to a postal or telecommunications operator and requires that operator to collect the data and provide it to the council.

6. Integral to the acquisition of communications data under RIPA, is the Single Point of Contact (SPoC). The role of the SPoC is to enable and maintain effective cooperation between a public authority and communications service providers in the lawful acquisition and disclosure of communications data. Any Notices or Authorisations must be passed to the service provider through a SPoC.

7. SPoCs must be properly trained in accordance with Home Office guidelines and must register their details with the Home Office.

8. The council currently uses the National Anti-Fraud Network (NAFN) as its SPoC.

Judicial Approval

1. Any grant of renewal of an authorisation for use of directed surveillance, use of covert human intelligence source or access to communications data, will need to be approved by order of a Justice of the Peace (District Judge or lay magistrate) before it can take effect.

2. Applicants will still need to ensure an authorisation is completed by and Authorising Officer before an application for Judicial Approval is made.

3. An application to the court should be made in good time before the start of the surveillance to be authorised. The court should be contacted to arrange a suitable hearing date and should be provided with:
    - A copy of the relevant authorisation
    - A written application for judicial approval
    - Any other relevant reference or supporting material relating to the application

4. Once an application date has been set, the applicant will appear before a Justice of the Peace (JP) in a private hearing. The JP will consider the application and may question the applicant to clarify certain points, or require additional reassurance on particular matters. The nature of the questioning will be for the JP to satisfy themselves that the surveillance is necessary and proportionate and has been through the proper approval process within the council.

5. In order to appear before a JP, the applicant will first need to be authorised by the Senior Responsible Officer to represent the council under s.223 of the Local Government Act 1972.

6. On hearing the application, the JP may decide to:
    - Approve the grant or renewal
    - Refuse to approve
    - Refuse to approve and quash the authorisation or notice

7. Further guidance on the judicial approval process can be found at www.homeoffice.gov.uk

Elected Members (Pursuant to Section 71 of the Regulation of Investigatory Powers Act 2000)

Elected Members of Hinckley & Bosworth Borough Council shall review the authority's use of the 200 Act and set the policy at least once a year to ensure that tit is being used consistently with the local authority's policy and that the policy remains fit for purpose. They should not, however, be involved in making decisions on specific authorisations.

Social media

Using social media for investigative purposes: October 2014; Review date: October 2016

Purpose

This policy aims to offer officers using social media sites for investigative purposes, guidance on how to do so in accordance with HBBC policy. An additional policy documented entitled Social Media Policy and Guidelines provides more general guidance in relation to using social media sites for non-investigative measures.

Scope

This policy is restricted to information being accessed through public open sources.

Definitions of social media

For the purpose of these guidelines, social media is held to include:

- Blogs (WordPress, Tumblr, Blogger)
- Micro blogging (Twitter)
- Forums
- Networks (Facebook, Ning, LinkedIn)
- File sharing sites (YouTube, Flickr)

Open Source Internet Intelligence sources

Open source intelligence sources are intelligence collected from publicly available sources. As such, investigative officers at HBBC, with permission from the Council's IT department, can search such sources for intelligence necessary to pursue their investigation. This **does not have to be obtained on a case-by-case basis**.

Officers must obtain authorisation from their line manager and head of service. This will then enable that officer with the relevant IT permissions and authority, to autonomously conduct appropriate intelligence gathering activities, where that officer considers that such intelligence gathering methods are appropriate, proportionate, reasonable and necessary in order to effectively investigate offences.

The following circumstances provide an example of when investigative officers might employ open sourced intelligence methods of investigation.

- To evidence information in relation to a fraud allegation such as housing or benefit fraud
- To support an anti-social behaviour complaint

The most common sources of open source investigation are social networking sites, search engines and auction sites, including:

- Facebook
- Friends Reunited
- Bebo
- Myspace
- Twitter
- EBay
- LinkedIn
- Google

(This list is not exhaustive)

Restrictions

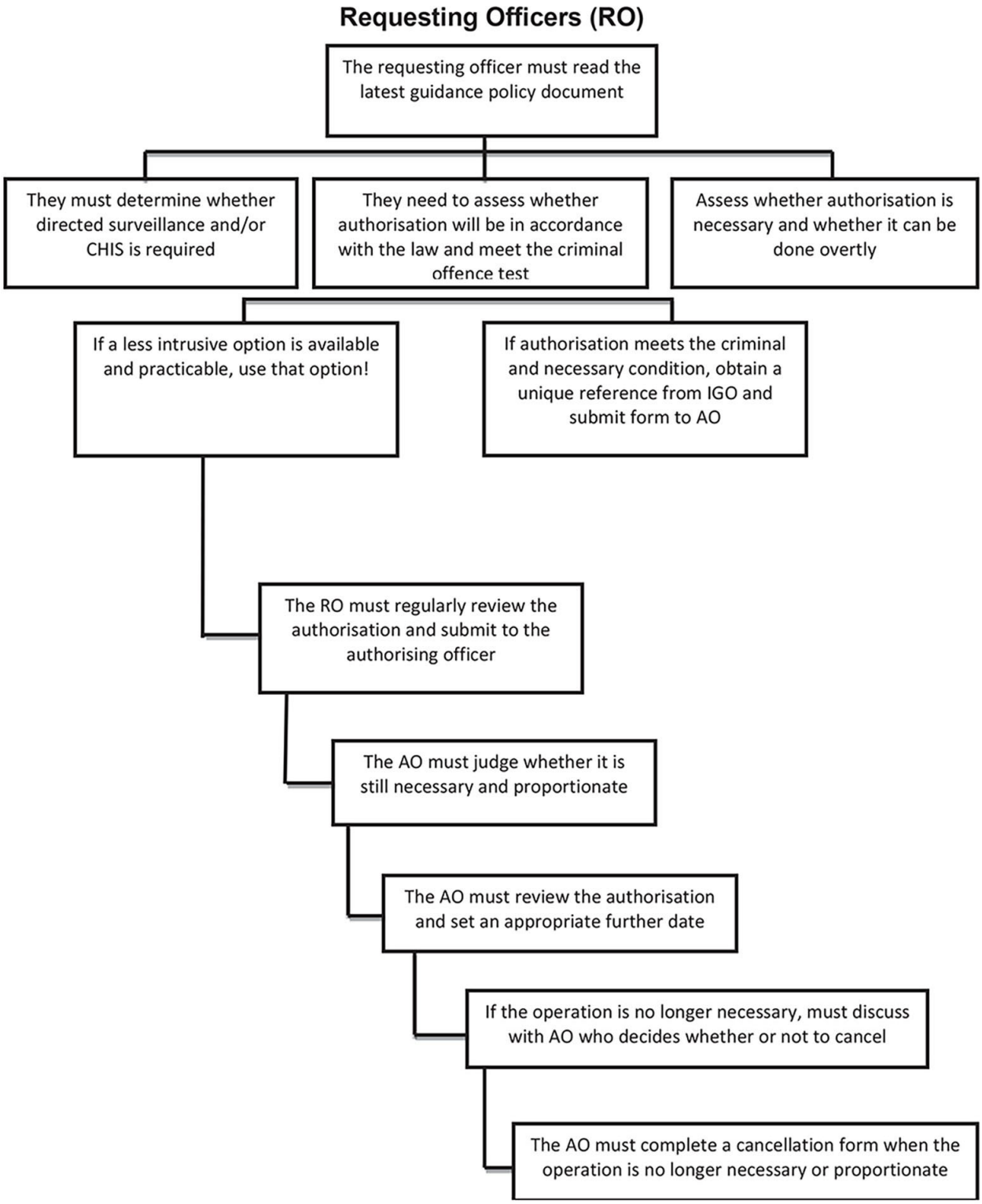
Officers accessing open sourced intelligence in this way **must not** attempt to view privately set profile information on social networking sites. Only publicly available information can be scrutinised.

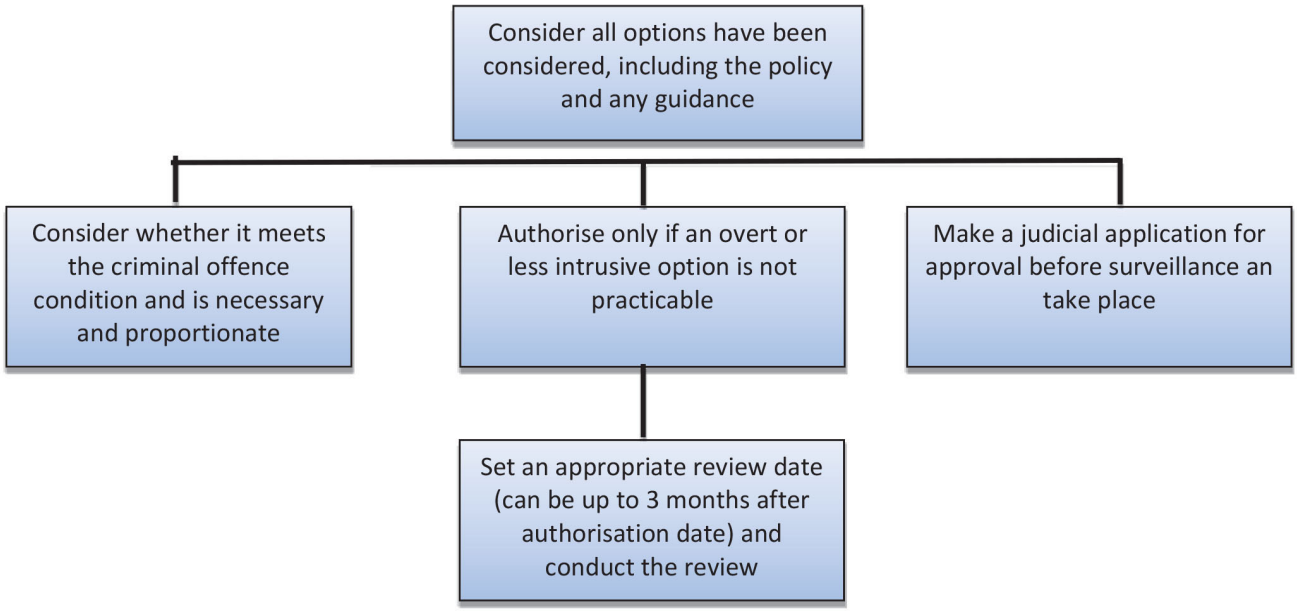
Officers must not add an investigation subject as a friend in order to access private information.

If valuable information is seen when a page is first checked, it is prudent to take screen shots at that time. Once contacted with regard to their cases (when asked to attend interview), customers can often change their privacy settings, meaning that officers are then unable to gather useful intelligence.

Any safeguarding issues should be reported in line with the council's safeguarding policy.

M RIPA Flowchart





Essential

RIPA flowchart - Authorising Officers

Send all authorised (and any rejected) forms, Judicial approval from court, review, renewals and cancellations to the Information Governance Officer (ICO) within **five working days of the relevant event**.

RIPA Authorising Officer Certificate

Hinckley & Bosworth Borough Council

I HEREBY CERTIFY that the officer whose personal details are given below is an Authorising Officer for the purposes of authorising covert surveillance and the use and/or conduct of Covert Human Intelligence Sources ('CHIS') under the provisions of the Regulation of Investigatory Powers Act 2000.

It is further certified that this officer has received training to perform such authorisation procedures.

Certificate issued to: (full name of officer)

Job title:

Service:

Location:

Certificate:

Date:

Signed: ……..

Bill Cullen, Chief Executive

Hinckley & Bosworth Borough Council

(PLEASE NOTE: This certificate and the authorisation granted by it is personal to the officer name in it and cannot be transferred. Any change in personal details must be notified in writing to the Chief Executive immediately. This certificate can be revoked at any time by the Chief Executive by written revocation issued to the officer concerned. It is the named officer's personal responsibility to ensure full compliance with RIPA authorisation and to ensure that s/he is fully trained in such procedures and that such training is kept up to date).