



# Buckinghamshire & Milton Keynes Fire Authority

<b>MEETING</b>	Fire Authority
<b>DATE OF MEETING</b>	18 February 2015
<b>OFFICER</b>	Graham Britten, Director of Legal and Governance
<b>LEAD MEMBER</b>	Councillor Adrian Busby
<b>SUBJECT OF THE REPORT</b>	<b>Annual Report on Regulation of Investigatory Powers Act 2000 (RIPA)</b>
<b>EXECUTIVE SUMMARY</b>	<p>The statutory guidance relating to RIPA requires that the Authority:</p> <ol style="list-style-type: none"> <li>1. Receive an update at least annually of the use by the Authority of surveillance and use of Covert Human Intelligent Sources (CHIS) (Annexes A and B).</li> <li>2. Have the opportunity to review the CHIS and Surveillance policy annually (Annex C).</li> </ol> <p>The Authority has had no requirement to use RIPA for enforcing the Regulatory Reform (Fire Safety) Order 2005 since the last report in February 2014.</p>
<b>ACTION</b>	Information.
<b>RECOMMENDATIONS</b>	<p>It is recommended that:</p> <ol style="list-style-type: none"> <li>i. the report be noted</li> <li>ii. the revised policy (annex C) be approved.</li> </ol>
<b>RISK MANAGEMENT</b>	<p>Non-compliance with RIPA could also result in non-compliance with the Data Protection Act (DPA). Under both RIPA and the DPA there are criminal and/or civil sanctions for breaches of personal information which may result in reputational and financial damage to the Authority.</p>
<b>FINANCIAL IMPLICATIONS</b>	None directly arising from the recommendations.
<b>LEGAL IMPLICATIONS</b>	<p>On 10 December 2014 revised versions of the two codes of practice under Part two of RIPA came into force as a result of two statutory instruments made on 19 November 2014:</p> <ul style="list-style-type: none"> <li>• the Regulation of Investigatory Powers (Covert Surveillance and Property Interference: Code of Practice) Order 2014</li> <li>• the Regulation of Investigatory Powers (Covert</li> </ul>

	Human Intelligence Sources: Code of Practice) Order 2014.
<b>HEALTH AND SAFETY</b>	None.
<b>EQUALITY AND DIVERSITY</b>	None.
<b>USE OF RESOURCES</b>	Maintaining a RIPA compliant policy and associated procedures involves periodic training for relevant staff to maintain competence.
<b>PROVENANCE SECTION &amp; BACKGROUND PAPERS</b>	<p>Background</p> <p>Since the introduction of RIPA (2000) there have been a number of amendments to the Act and related Codes of Practice. These are reported to the Authority, at least, annually to note and to request approval to policy changes. In 2009 Fire and Rescue Services were consulted as to whether to maintain their status as "listed bodies" <a href="#">Fire Service Circular FRSC29 2009</a>. The decision to maintain listed body status means that the Authority must ensure that it has adequate relevant policies and procedures in place.</p> <p>Background papers</p> <ul style="list-style-type: none"> <li>• <a href="#">Annual RIPA report 18 April 2012</a>, Item 8.</li> <li>• <a href="#">Office of Surveillance Commissioner's Inspection Report. Executive Committee 8 August 2012</a> Item 15.</li> <li>• <a href="#">Code of practice for the interception of communications</a> (8 September 2010)</li> <li>• <a href="#">Code of practice for investigation of protected electronic information</a> ( 8 September 2010)</li> <li>• <a href="#">Code of practice for the acquisition and disclosure of communications data</a> (8 September 2010)</li> <li>• <a href="#">Interception of communications: code of practice</a> (12 March 2010)</li> <li>• <a href="#">Covert Human Intelligence Source Code of Practice</a></li> <li>• <a href="#">Regulation of Investigatory Powers (Juveniles) Order 2000</a></li> <li>• <a href="#">The Regulation of Investigatory Powers (Covert Human Intelligence Sources: Code of Practice)</a></li> </ul>

	<p><a href="#">Order 2014.</a></p> <ul style="list-style-type: none"> <li>• <a href="#">Regulation of Investigatory Powers 2000</a></li> <li>• <a href="#">Chief Surveillance Commissioner's annual report 28 September 2014</a></li> </ul> <p>Since the last report (19 February 2014), revised versions of the two codes of practice under <a href="#">Part 2 of the Regulation of Investigatory Powers Act 2000</a> came into force (10th December 2014):</p> <ul style="list-style-type: none"> <li>• <a href="#">The Regulation of Investigatory Powers (Covert Surveillance and Property Interference: Code of Practice) Order 2014</a> and</li> <li>• <a href="#">the Regulation of Investigatory Powers (Covert Human Intelligence Sources: Code of Practice) Order 2014.</a></li> </ul> <p>and the Home Office has introduced a <a href="#">Surveillance Camera Code of Practice (June 2013)</a>. The ICO has also revised its CCTV Code of Practice <a href="#">In the picture: A data protection code of practice for surveillance cameras and personal information</a> to ensure that authorities use surveillance cameras lawfully.</p> <p>There is also an extensive list of other changes that Sam Lincoln (Chief Surveillance Inspector 2006 – 2013) has noted in a recent article (posted 5 January 2015). Annex B is based on this article.</p> <p><a href="https://actnowtraining.wordpress.com/2015/01/05/the-new-ripa-surveillance-codes-key-changes/">https://actnowtraining.wordpress.com/2015/01/05/the-new-ripa-surveillance-codes-key-changes/</a></p>
<b>APPENDICES</b>	<p>Annex A: RIPA Update.                  Annex B: BMKFA CHIS and Surveillance Policy                  Annex C: The changes to the Codes of Practice</p>
<b>TIME REQUIRED</b>	5 minutes.
<b>REPORT ORIGINATOR AND CONTACT</b>	<p>Gerry Barry, Information Governance and Compliance Manager  <a href="mailto:gbarry@bucksfire.goc.uk">gbarry@bucksfire.goc.uk</a>                  01296 744442 or 07920 710637</p>

## **Annex A RIPA Update**

In recent years there have been a number of changes in legislation to reflect concerns as to the misuse of surveillance systems and other intrusive technologies.

The Home Office: Surveillance Camera Code of Practice (2013) governs the use of surveillance camera systems including CCTV and Automatic Number Plate Recognition (ANPR).

The Information Commissioner's Office (ICO) has also published its revised code of practice on CCTV (October 2014) which aims to reflect the developments in technologies that have taken place since the 2008 revision and explain the impact that case law has had on this area of surveillance systems.

In the Chief Surveillance Commissioner's annual report (September 2014) he drew attention to the use of the Internet for investigations; particularly involving social networking sites, and suggests that a RIPA authorisation may be required for some online investigations.

On 10 December 2014 revised versions of the two codes of practice under Part 2 of the Regulation of Investigatory Powers Act 2000 (RIPA) came into force:

- The Regulation of Investigatory Powers (Covert Human Intelligence Sources: Code of Practice) Order 2014 and
- The Regulation of Investigatory Powers (Covert Surveillance and Property Interference: Code of Practice) Order 2014.

Paragraph 2.29 of the revised covert surveillance code states:

*"The use of the internet may be required to gather information prior to and/or during an operation, which may amount to directed surveillance. Whenever a public authority intends to use the internet as part of an investigation, they must first consider whether the proposed activity is likely to interfere with a person's Article 8 rights, including the effect of any collateral intrusion. Any activity likely to interfere with an individual's Article 8 rights should only be used when necessary and proportionate to meet the objectives of a specific case. Where it is considered that private information is likely to be obtained, an authorisation (combined or separate) must be sought as set out elsewhere in this Code. Where an investigator may need to communicate covertly online, for example contacting individuals using social media websites, a CHIS authorisation should be considered."*

Paragraph 4.32 of the revised CHIS code states:

*"The use of the internet may be required to gather information prior to and/or during a CHIS operation, which may amount to directed surveillance. Alternatively the CHIS may need to communicate online, for example this may involve contacting individuals using social media websites. Whenever a public authority intends to use the internet as part of an investigation, they must first consider whether the proposed activity is likely to interfere with a person's Article 8 rights, including the effect of any collateral intrusion. Any activity likely to interfere with an individual's Article 8 rights should only be used when necessary and proportionate to meet the objectives of a specific case. Where it is considered that private information is likely to be obtained, an authorisation (combined or separate) must be sought as set out elsewhere in this Code."*

## **Annex B The New RIPA Surveillance Codes: Key Changes**

The revised codes implement the amendments to RIPA resulting from the legislation enacted since the last codes were published namely: the Regulation of Investigatory Powers (Extension of Authorisation Provisions: Legal Consultations) Order 2010; to the Protection of Freedoms Act 2012; and the Regulation of Investigatory Powers (Covert Human Intelligence Sources: Relevant Sources) Order 2013. There are some other important changes.

### **Covert Surveillance and Property Interference Code**

**N.B.** Please note paragraphs numbers in square brackets ([ ]) refer to the paragraph numbering in the Code of Practice:

[2.18] The first sentence is amended to account for the fact that some legal consultations which might otherwise be Directed Surveillance are now to be authorised as Intrusive Surveillance.

[2.24] Examples 3 and 4 have been amended. Applicants are reminded of [1.7] "Examples are included in this code to assist with the illustration and interpretation of certain provisions..."

[2.27] This paragraph has been expanded to include guidance provided by the Surveillance Camera Code of Practice pursuant to the Protection of Freedoms Act.

[2.29] This new paragraph provides important guidance regarding the need to consider whether an authorisation for either Directed Surveillance or a CHIS is required when using the Internet.

[2.30] The third bullet point of this paragraph is amended to differentiate between non-verbal and verbal noise.

[3.7] The original examples 2 and 3 are deleted.

[3.18] This is a new paragraph and covers the use of third party individuals or organisations (for example private investigators and internet researchers). They are acting as agents of the public authority and the need for relevant authorisation must not be ignored.

[3.22] The deletion of reference to Scottish public authorities.

[3.30 - 3.33] These new paragraphs cover the changes to local authority authorisations of Directed Surveillance resulting from the Protection of Freedoms Act 2012.

[3.35] This paragraph amends the requirement for elected members to consider internal reports submitted on a 'regular basis' rather than at least quarterly.

[4.1] The fourth sentence is amended slightly so that the definition of a Member of Parliament is deleted and placed in the glossary at the back of the code.

[5.18] Advises that there is no 'legal' requirement for any further details to be recorded.

[5.20] The footnotes relating to this paragraph have been deleted.

[6.2] Is amended to include directed surveillance.

[8.1] An additional sentence is added directing local authorities to the gov.uk website for further guidance on the recording of magistrates' decisions.

[8.2] A final bullet is included requiring local authorities to retain a copy of the Magistrates' approval order in a centrally retrievable form.

[8.4] This is a new paragraph advising that it is desirable that relevant records should be retained, if possible, for up to five years.

### **CHIS Code of Practice**

[2.4] This alerts the renaming of CHIS previously known as undercover officers to 'relevant source'.

[2.12] The final sentence of this paragraph is an important amendment. It alerts public authorities to the fact that the existence of a CHIS is not a choice for a public authority. All public authorities must acknowledge that a CHIS may appear at any time and must have procedures in place to manage them in accordance with the law.

[2.14] This new paragraph obliges 'relevant sources' to comply with the College of Policing Code of Ethics.

[2.15] This is a new paragraph obliging the authorisation of activity known as 'legend building'.

[2.16] This new paragraph notes that not all human source activity will meet the definition of CHIS.

[2.17] This new paragraph introduces the concept of a public volunteer in addition to the previously existing concept of a human source with a professional or statutory duty.

[3.12] This paragraph is amended in recognition that the 2013 Order introduced enhanced arrangements.

[3.22] The amendment to this paragraph emphasises that the enhanced arrangement for relevant sources relies on accurate recording of the length of deployment of each relevant source.

[3.26 – 3.27] This new section is specific to the use of CHIS by local authorities and the approval by magistrates. It highlights differences between authorities in England and Wales, Scotland, and Northern Ireland. Similar direction is provided to the need for elected member review.

[4.3] A reminder that 'relevant sources' are subject to enhanced arrangements when accessing legally privileged and other confidential information.

[4.31] There is an addition to cover the engagement of a member of a foreign law enforcement agency.

[4.32] There is an important new paragraph covering the considerations necessary to authorise the use and conduct of a CHIS for some online covert activity. It should be read in conjunction with [2.29] of the Covert Surveillance and Property Interference Code of Practice.

[5.10] This new paragraph clarifies the enhanced arrangements for relevant sources.

[5.15] Two sentences are added to this paragraph. The first states that local authorities are no longer able to orally authorise the use of RIPA techniques. The second relates to out of hours arrangements.

[5.16] Amended to introduce additional information to include at review; namely the information obtained from a CHIS and the reasons why executive action is not possible if that is the case.

[5.21 and 5.22 – 5.26] These new paragraphs relate to enhanced arrangements for the use and conduct of relevant sources. They provide detail regarding timings and, importantly, the calculation of total or accrued deployment or cumulative authorisation periods.

[5.29] Additional sentence requiring an Authorising Officer to satisfy themselves that all welfare issues are addressed at the time of CHIS cancellation.

[5.30 – 5.31] These new paragraphs relate to the refusal of an Ordinary Surveillance Commissioner to approve a long term authorisation. Importantly, it obliges public authorities to plan for the safe extraction of a relevant source if an authorisation is refused.


[6.6] Adds a final sentence recognising concerns raised by the Office of the Surveillance Commissioner in relation to traditional police appointments and their responsibilities as defined by RIPA.

[7.3] Similar to [8.4] of the Covert Surveillance and Property Interference Code revision, this new paragraph (and amendment of [7.1] and [7.6]) recommends that relevant RIPA records should be retained for five years if possible.

[7.6] The addition of a bullet point requires that the decision of an Ordinary Surveillance Commissioner should be retained.

**Based on the Act Now article by Sam Lincoln (Chief Surveillance Inspector 2006 – 2013)**

**Annex C CHIS and Surveillance Policy**

	<b>Information Asset Owner:</b>	<b>Director of Legal &amp; Governance</b>
	<b>Page :</b>	<b>1 of 9</b>
<b>Policy Note: CHIS and Surveillance Policy</b>		

**1. Record history**

- 1.0 First issue
- 2.0 Amended to reflect changes in legislation
- 3.0 Amended to reflect changes in legislation that came into effect in December 2014 (highlighted in yellow).

**Index**

- 2. Introduction .....2
- 3. Purpose.....2
- 4. Access to communication data .....2
- 5. Implementation .....2
- 6. Basic requirements .....2
- 7. Types of surveillance.....3
- 8. Authorisation and duration ..... 3
- 9. Authorising Officer .....3
- 10. Evidence .....3
- 11. Covert human intelligence sources (CHIS).....4
- 12. Chis .....4
- 13. Management of the source .....5
- 14. Record keeping .....6
- 15. Safety & security.....7
- 16. Annual review .....7



## **2. Introduction**

- 2.1 Some Authority activities may require the use of covert surveillance as part of its enforcement functions. The Regulation of Investigatory Powers Act 2000 (RIPA) provides the statutory framework for the granting of authority to carry out surveillance.
- 2.2 The Authority is fully committed to complying with the Human Rights Act 1998 (HRA) and the Regulation of Investigatory Powers Act 2000 (RIPA). To ensure compliance, all covert surveillance and use of covert human intelligence source (CHIS), falling within the scope of the Act carried out by officers of the Authority, must be authorised by a designated 'Authorising Officer'.
- 2.3 In complying with RIPA, officers must have full regard to the Code of Practices issued by the Home Office which can be found at:
  - [Code of practice for the interception of communications](#)
  - [Code of practice for investigation of protected electronic information](#)
  - [Code of practice for the acquisition and disclosure of communications data](#)
  - [Code of Practice for the use of Human Intelligence Sources](#)

## **3. Purpose**

The purpose of this document is to set out the Authority's policy on RIPA, reinforce the requirements of the Act, the Order and Codes of Practice, provide guidance to officers, protect the rights of individuals and minimise the risk of legal challenge as a result of officer actions.

## **4. Access to communication data**

- 4.1 The Authorities investigating criminal offences have powers (by virtue of The Regulation of Investigatory Powers (Communications Data) Order 2004 ("the Order")) to gain access to information held by telecommunication or postal service providers about the use of their services by persons who are the subject of criminal investigations.

## **5. Implementation**

- 5.1 On approval, this policy will be published on the Authority intranet, supporting procedures will be updated and also published on the Authority intranet and other training rolled out to officers, proportionate to their role, as required.

## **6. Basic requirements**

- 6.1 Under RIPA, the Order and Codes of Practice, directed covert surveillance, use of CHIS and access to communications data should only be authorised if the Authorising Officer is satisfied that:
  - a) The action is necessary for the prevention or detection of crime or the prevention of disorder.
  - b) The surveillance/access to communications data is proportionate. A measure or action is 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 considerations.

c) Three essential elements must be met:

- the proposed covert surveillance is proportional to the mischief under investigation;
- is proportional to the degree of anticipated intrusion on the target and others; and
- is the only option, other overt means having been considered and discounted.

## **7. Types of surveillance**

- 7.1 Covert surveillance is surveillance that is carried out in a manner to ensure that the persons subject to the surveillance are unaware that it is or may be taking place. Surveillance may be 'directed' or 'intrusive'.
- 7.2 The Authority is not authorised to conduct Intrusive Surveillance, or to interfere with the property of others whilst conducting directed surveillance.
- 7.3 Intrusive surveillance – is carried out in relation to anything taking place on any residential premises or in any private vehicle by an individual on the premises or in the vehicle or is carried out by means of a surveillance device. Although a surveillance device not on or in the premises/vehicle will only be intrusive if it consistently provides information of the same quality and detail as might be expected to be obtained for a device actually on/in the premises/vehicle.
- 7.4 Directed surveillance – is covert, but not intrusive and is undertaken for the purposes of a specific investigation or operation and involving the observation of a person or persons in order to gather private information about them (which can include information about persons at work). Covert surveillance includes monitoring, observing or listening to persons without their knowledge.
- 7.5 Deciding when authorisation under RIPA is required involves making a judgement. Where surveillance is covert and is directed at individual(s) to obtain information about them, RIPA is likely to apply and prior authorisation obtained in accordance with this policy.
- 7.6 Directed surveillance must be authorised, in accordance with this policy, and only be used for legitimate purposes, when sufficient evidence exists and documented to warrant the exercise and when surveillance is shown to be both the least harmful means of meeting that purpose and proportionate to what it seeks to achieve.
- 7.7 It is imperative that all reasonable alternative methods to resolve a situation, such as naked-eye observation, interview or changing methods of working or levels of security should be attempted first and recorded in writing with the reason for surveillance being requested fully documented. Where the subject of covert surveillance is an employee, the Authority's Legal Officer (the Director of Legal & Governance) must be informed.

## **8. Authorisation and duration**

- 8.1 All requests to conduct, extend or discontinue a covert surveillance exercise must be made in writing on the appropriate forms. All requests must be submitted to the Authorising Officer. All requests and extensions must be considered and authorised in writing, by the Authorising Officer, before any covert surveillance operation can commence or continue.
- 8.2 Authorisation can only be granted where covert surveillance is believed, by the Authorising Officer, to be necessary and proportionate. Written authorisations for direct covert surveillance will be valid for 3 months from the date of the original authorisation or extension, the Authorising Officer is responsible for ensuring that surveillance is cancelled as soon as it is no longer required.
- 8.3 if during the investigation it becomes clear that the activity being investigated does not amount to a criminal offence or that it would be a less serious offence that does not meet the threshold the use of directed surveillance should cease. If a directed surveillance authorisation is already in force it should be cancelled.
- 8.4 Applications for renewals should not be made until shortly before the original authorisation period is due to expire but the Authority must take account of factors which may delay the renewal process (e.g. intervening weekends or the availability of the relevant Authorising Officer).

## **9. Authorising Officer**

The Authorising Officer will be a post holder in the role of Group Manager or above.

## **10. Evidence**

- 10.1 During a covert operation, recorded material or information collected will be stored and transported securely. It will be reviewed regularly (at least weekly) and access to it will be restricted to the Authorising Officer and the Enforcement Officers concerned.
- 10.2 The Authorising Officer will decide whether to allow requests for access by third parties. Access will generally only be allowed to limited and prescribed parties including law enforcement agencies, prosecution agencies, legal representatives and the people subject to the surveillance (unless disclosure would prejudice any criminal enquiries or proceedings). Authorising Officers will maintain a record of all reviews of material recorded and collected covertly.
- 10.3 Once a covert operation results in an individual being under suspicion of having committed a criminal offence, he/she must be informed of this as promptly as is reasonably practicable if the fire authority is pursuing the offences. This is in order to ensure their right to a fair trial or hearing within a reasonable time in accordance with the Human Rights Act.
- 10.4 In a situation where it is considered that a matter gives rise to a potential criminal prosecution, any interview with the suspect must be 'under caution' and conducted by a suitably trained officer.

## **11. Covert human intelligence sources**

- 11.1 A person is a CHIS if they:

- a) establish or maintain a personal or other relationship with a person for the covert purpose of facilitating the doing of anything falling within paragraphs (b) or (c) below;
- b) covertly use such a relationship to obtain information or to provide access to any information to another person; or
- c) covertly disclose information obtained by the use of such a relationship or as a consequence of the existence of such a relationship.

11.2 A CHIS may be required to establish or maintain a personal or other relationship for a covert purpose, i.e. one which the person with whom the relationship is established is unaware of. A CHIS is "tasked" to obtain information, provide access to information or to otherwise act, incidentally, for the benefit of the Authority. Authorisation for the use or conduct of a CHIS is required prior to any tasking where such tasking requires the source to establish or maintain a personal or other relationship for a covert purpose.

11.3 The Code of Practice strongly recommends that the Authority consider an authorisation whenever the use or conduct of CHIS is likely to engage an individual's rights under Article 8, whether this is through obtaining information, particularly private information, or simply through the covert manipulation of a relationship. An authorisation will be required if a relationship exists between the subject and the CHIS, even if specific information has not been sought by the Authority.

11.4 However, the provisions of the 2000 Act do not 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. Members of the public acting in this way would not generally be regarded as sources. A routine test purchase which does not go beyond a normal transaction is unlikely to be considered a CHIS activity.

11.5 The use of CHIS by the Authority is likely to be infrequent. A judgement must be made in determining when an individual taking part in an investigation may be acting as a CHIS and if in any doubt, should seek advice from the Authorising Officer.

## **12. Chis authorisation**

12.1 The same principles and procedures apply for the authorisation of CHIS as for directed surveillance. The Authorising Officer may authorise the use of CHIS if they are satisfied that it is necessary and proportionate to do so, and arrangements are in place for managing a CHIS.

12.2 Applications to use, extend or discontinue the use of CHIS must be made in writing.

12.3 Written authorisations for CHIS will be valid for 12 months from the date of authorisation or extension. Exceptionally, an oral authorisation may be granted for the use of a CHIS in circumstances of urgency.

12.4 An oral authorisation will be valid for 72 hours but will be subject to the same requirements as that set out in part 2 relating to urgent authorisations for directed surveillance. As with directed surveillance, the Authorising Officer is responsible for ensuring that authorisation is cancelled as soon as it is no longer

required, and that reviews of authorisations are carried out on at least a monthly basis.

- 12.5 There are additional considerations which must be taken into account before the use of a CHIS can be authorised. These relate to the security, welfare and management of the source and records relating to his/her use. Details of these issues are set out in paragraphs 14.1 – 14.3 below.
- 12.6 Material obtained from a CHIS may be used as evidence in criminal proceedings and the proper authorisation of a CHIS should ensure the legality of such evidence.
- 12.7 Before authorising the use of a CHIS, the Authorising Officer and Enforcing Officers must ensure that, as far as is possible, measures are taken to avoid unnecessary intrusion into the lives of those not directly connected with the investigation.
- 12.8 An authorisation for a CHIS may be in broad terms and highlight the nature of the CHIS's task. However, where it is intended to task a source in a new or significantly greater way, the handler or controller must refer the proposed tasking to the Authorising Officer, who should consider whether a separate authorisation is required.

### **13. Management of the source**

- 13.1 The Authorising Officer must not grant an authorisation for the use or conduct of a source unless he/she has appointed a person who is responsible for having day to day contact with the source, and a person with the responsibility for the general oversight of the use of the source.
- 13.2 The person with day to day responsibility will be a 'Handler' and will deal with the CHIS on behalf of the Authority, direct the day to day activities of the CHIS, record the information supplied by him/her and monitor the security and welfare of the CHIS. Meetings with the source must be recorded, along with details of meeting between the source and the subject of the investigation. Where there are unforeseen occurrences, these should be recorded as soon as practicable after the event, and the authority checked to ensure that it covers the circumstances that have arisen.
- 13.3 The person with the general oversight of the CHIS will be a 'Controller'.

### **14. Record keeping**

- 14.1 The Regulation of Investigatory Powers (Source Records) Regulations 2000 provides that the following records must be kept when a CHIS is authorised:
- The identity of the source.
  - The identity, where known, used by the source.
  - Any relevant investigating authority, other than the Authority, maintaining the records.
  - The means by which the source is referred to within each relevant investigating authority.

- Any other significant information connected with the security and welfare of the source.
- Any confirmation made by a person granting or renewing an authorisation for the conduct or use of a source that relevant information has been considered and that any identified risks to the security and welfare of the source have where appropriate been properly explained to and understood by the source.
- The date when, and the circumstances in which, the source was recruited.
- The identifies of the persons who will act as handler, controller and person responsible for maintaining records of the use of the source.
- The periods during which those persons have discharged those responsibilities.
- The tasks given to the source and the demands made of him in relation to his activities as a source.
- All contacts or communications between the source and the authority's handler.
- The information obtained by the authority by the conduct or use of the source.
- Any dissemination by that authority of information obtained in that way.
- Any payment benefit or reward made or provided to the source (other than where the source is an authority employee acting as an undercover operative).

14.3 The Code of Practice on the use of CHIS also contains additional advice on records to be kept in relation to a source. In addition to the authorisation forms, risk assessment, and the above information, a record should be kept of the circumstances in which tasks were given to the source and the value of the source to the authority.

14.4 The records must be kept in a way that preserves the confidentiality of the source and the information provided by him/her. Records must not be made available to officers unless it is necessary for them to do so.

14.5 The Authorising Officer must not authorise the use of a CHIS until an appropriate officer has been designated as the person with responsibility for maintaining a record of the use made of the CHIS, and arrangements are in place for ensuring that the records will be kept securely.

14.6 All records will be protectively marked, in accordance with the Authority Protective Marking Scheme, to assist in protecting their confidentiality.

## **15. Safety & security**

15.1 Prior to the authorising of a CHIS, the Authorising Officer shall have regard to the safety and welfare of the CHIS and shall continue to have such regard, throughout the use of the CHIS. The safety and welfare of the CHIS after the authorisation has been cancelled or where the investigation has been closed must also be taken into account at the outset. Officers seeking authorisation to use a CHIS must consider the corporate risks to determine the risk to the source of any tasking and the likely consequences should the role of the source become known. The nature and magnitude of risk to the source must be identified and evaluated. Risk on a personal, operational and ethical basis must be considered.

These risk assessments must be taken into account by the Authorising Officer in deciding whether it is appropriate for authorisation to be granted for the use of the CHIS, along with the usual considerations of proportionality, necessity etc. The Authorising Officer must satisfy him/herself that any risks identified are justified in relation to the investigation, and that any identified risks have been properly explained and understood by the source. A copy of the risk assessment must be kept in accordance with the preceding paragraph.

15.2 The handler of the CHIS will be responsible for bringing any concerns about the personal circumstances of the source to the attention of the controller, in so far as they may affect the validity of the risk assessment, the conduct of the source and the safety and welfare of the source. Where appropriate such concerns should be brought to the attention of the Authorising Officer and a decision taken on whether or not to allow the authorisation to continue.

15.3 The use of vulnerable individuals or juveniles for a CHIS purpose must only be authorised by the Chief Fire Officer/ Chief Executive or the Chief Operating Officer and only in the most exceptional cases. The Authorising Officer must also abide by the Code of Practice relating to juveniles. On no account should the use or conduct of a source under 16 years of age be authorised to give information where the relationship to which the use of the source relates is between the source and his parents or any person who has parental responsibility for him. In other cases authorisation should not be granted unless the special provisions contained within the Regulation of Investigatory Powers (Juveniles) Order 2000 are satisfied. These requirements relate to the presence of an appropriate adult (e.g. a parent) at meetings with the source and consideration of risk assessments. Authorisation of juvenile CHIS may only be granted by the Chief Fire Officer/ Chief Executive or the Chief Operating Officer (or equivalent) and the duration of such an authorisation will be only one month, rather than twelve months.

## **16. Annual review**

16.1 The Authority should review use of RIPA and set the policy at least once a year. They should also consider internal reports on use of the 2000 Act **on a regular basis** to ensure that it is being used consistently with the policy and that the policy remains fit for purpose. They should not, however, be involved in making decisions on specific authorisations.

This page is left intentionally blank