 Buckinghamshire & Milton Keynes Fire Authority MAKING YOU SAFER PREVENTING PROTECTING RESPONDING WWW.BUCKSFIRE.GOV.UK	Information Asset Owner:	Chief Operating Officer Directorate
	Protective Marking:	PROTECT
	Page :	1 of 12
Policy Note: 80-001-002		CHIS and Surveillance Policy


To:	Document Type:	✓	Document Summary:
All employees	Policy	✓	The purpose of this document is to set out the Service policy and procedures on RIPA, to reinforce the requirements of the Act, the Order and Home Office Codes of Practice. This document also provides guidance to nominated officers, protects the rights of individuals and minimises the risk of legal challenge as a result of nominated officers' actions
	Assessment		
	Procedure		
	Guidance Note		
	Technical Note		
	Information		
	Safety Critical		

Keyword: each divided by commas

Please note that as Documents are frequently updated, if you print a document, its accuracy cannot be guaranteed, always check for latest version.

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

Version:	4.2	Status of document:	Draft
Author:	Response Policy	PIA:	N/A
Issue Date:	20 th December 2013	Review Date:	20 th December2014
File Name	BFRSD510100x		

 <p>Buckinghamshire & Milton Keynes Fire Authority MAKING YOU SAFER PREVENTING PROTECTING RESPONDING WWW.BUCKSFIRE.GOV.UK</p>	Information Asset Owner:	Chief Operating Officer Directorate
	Protective Marking:	PROTECT
	Page :	2 of 12
Policy Note: 80-001-002		CHIS and Surveillance Policy

1. Introduction

- 1.1 Some of the Buckinghamshire & Milton Keynes Fire Authority's (The Authority) activities may require covert surveillance as part of its enforcement functions. The Regulation of Investigatory Powers Act 2000 provides the statutory framework for the granting of authority to carry out surveillance.
- 1.2 The Authority is fully committed to complying with the Human Rights Act 1998 (HRA) and the Regulation of Investigatory Powers Act 2000 (RIPA – the Act). 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' in the form prescribed in the procedure note.
- 1.3 In complying with RIPA, officers must have full regard to the Code of Practices issued by the Home Office.


2. Purpose of the policy

- 2.1 It is essential that all activities of this nature, whether they will lead to prosecution or not, are carried out in accordance with the RIPA Codes of Practice and this policy. Investigations which fall within the scope of the Act, which are not authorised, could leave the authority vulnerable to legal challenge by individuals who consider that there has been an intrusion into their privacy.
- 2.2 The purpose of this document is to set out the authority's policy on RIPA, to reinforce the requirements of the Act the Order and Codes of Practice, to provide guidance to officers and to protect the rights of individuals and to minimise the risk of legal challenge as a result of officer actions.
- 2.3 Each investigation where the use of covert surveillance, CHIS or access to communications data is requested it must be subject to a separate authorisation request.

3. Access to communication data

- 3.1 In addition, local authorities investigating criminal offences now have powers (by virtue of The Regulation of Investigatory Powers (Communications Data)

Version:	4.2	Status of document:	Draft
Author:	Response Policy	PIA:	N/A
Issue Date:	20 th December 2013	Review Date:	20 th December 2014
File Name	BFRSD510100x		

 <p>Buckinghamshire & Milton Keynes Fire Authority MAKING YOU SAFER PREVENTING PROTECTING RESPONDING WWW.BUCKSFIRE.GOV.UK</p>	Information Asset Owner:	Chief Operating Officer Directorate
	Protective Marking:	PROTECT
	Page :	3 of 12
Policy Note: 80-001-002		CHIS and Surveillance Policy

Order 2004 ("the Order") to gain access to communications data – that is, information held by telecommunication or postal service providers about the use of their services by persons who are the subject of criminal investigations.

- 3.2 In using such powers, officers must have full regard to the Code of Practice on Accessing Communications Data, issued by the Home Office. As with covert surveillance, access to communications data must be authorised by a designated 'Authorising Officer'.


4. Implementation

- 4.1 The policy is operational forthwith.
- 4.2 A copy of this Policy Document together with the Home Office Codes of Practice and Investigatory Powers Tribunal leaflets will be made available for Public Inspection at Service Headquarters.

5. Basic requirements

- 5.1 Under the Act, the Order and Home Office 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 (in a democratic society) 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 are met:

Version:	4.2	Status of document:	Draft
Author:	Response Policy	PIA:	N/A
Issue Date:	20 th December 2013	Review Date:	20 th December 2014
File Name	BFRSD510100x		

 <p>Buckinghamshire & Milton Keynes Fire Authority MAKING YOU SAFER PREVENTING PROTECTING RESPONDING WWW.BUCKSFIRE.GOV.UK</p>	Information Asset Owner:	Chief Operating Officer Directorate
	Protective Marking:	PROTECT
	Page :	4 of 12
Policy Note: 80-001-002		CHIS and Surveillance Policy

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

6. Training

6.1 All enforcing officers and the Authorising Officer are trained on the provisions of RIPA, to ensure that the requirements of the law are complied with.

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 Local Authorities are 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.

Version:	4.2	Status of document:	Draft
Author:	Response Policy	PIA:	N/A
Issue Date:	20 th December 2013	Review Date:	20 th December 2014
File Name	BFRSD510100x		


 <p>Buckinghamshire & Milton Keynes Fire Authority MAKING YOU SAFER PREVENTING PROTECTING RESPONDING WWW.BUCKSFIRE.GOV.UK</p>	Information Asset Owner:	Chief Operating Officer Directorate
	Protective Marking:	PROTECT
	Page :	5 of 12
Policy Note: 80-001-002		CHIS and Surveillance Policy

- 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 document. If in doubt, seek authorisation.
- 7.6 Directed surveillance must be authorised in accordance with this policy and must only be used for legitimate purposes, and only when sufficient evidence exists and has been 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 extremely important 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 and the reason for surveillance being requested fully documented. Where the subject of covert surveillance is an employee, the Authority's Legal Officer 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, in accordance with the procedure document BFRSD 80-002-007. All such requests must be submitted to the Authorising Officer. All requests and extensions must be considered, authorised in writing by the Authorising Officer, before any covert surveillance operation can commence or continue.
- 8.2 Authorisation will 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, and for ensuring that reviews of authorisation are carried out on at least a monthly basis.
- 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

Version:	4.2	Status of document:	Draft
Author:	Response Policy	PIA:	N/A
Issue Date:	20 th December 2013	Review Date:	20 th December 2014
File Name	BFRSD510100x		

 <p>Buckinghamshire & Milton Keynes Fire Authority MAKING YOU SAFER PREVENTING PROTECTING RESPONDING WWW.BUCKSFIRE.GOV.UK</p>	Information Asset Owner:	Chief Operating Officer Directorate
	Protective Marking:	PROTECT
	Page :	6 of 12
Policy Note: 80-001-002		CHIS and Surveillance Policy

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 local authority authorising officer and a JP to consider the application).


9. Authorising officer

- 9.1 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.

Version:	4.2	Status of document:	Draft
Author:	Response Policy	PIA:	N/A
Issue Date:	20 th December 2013	Review Date:	20 th December 2014
File Name	BFRSD510100x		

 <p>Buckinghamshire & Milton Keynes Fire Authority MAKING YOU SAFER PREVENTING PROTECTING RESPONDING WWW.BUCKSFIRE.GOV.UK</p>	Information Asset Owner:	Chief Operating Officer Directorate
	Protective Marking:	PROTECT
	Page :	7 of 12
Policy Note: 80-001-002		CHIS and Surveillance Policy

11. Covert human intelligence sources

11.1 Definition – A person is a CHIS if :

- a) They 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) They covertly use such a relationship to obtain information or to provide access to any information to another person; or
- c) they 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 relevant public 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 However, the provisions of the 2000 Act 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. 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.

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

12. Chis authorisation

12.1 The same principles and procedures apply for the authorisation of a CHIS as for directed surveillance (see section 5 & 8). The Authorising Officer may authorise the use of a CHIS, provided that they are satisfied that it is


Version:	4.2	Status of document:	Draft
Author:	Response Policy	PIA:	N/A
Issue Date:	20 th December 2013	Review Date:	20 th December 2014
File Name	BFRSD510100x		

 <p>Buckinghamshire & Milton Keynes Fire Authority MAKING YOU SAFER PREVENTING PROTECTING RESPONDING WWW.BUCKSFIRE.GOV.UK</p>	Information Asset Owner:	Chief Operating Officer Directorate
	Protective Marking:	PROTECT
	Page :	8 of 12
Policy Note: 80-001-002		CHIS and Surveillance Policy

necessary and proportionate to do so, and that there are arrangements in place (set out below) for managing a CHIS.

- 12.2 Applications to use, extend or discontinue the use of a CHIS must be made in writing on the Fire Authority's corporate forms, as set out in the procedure document BFRSD 80-002-007.
- 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 15.1 – 15.3 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 (see below) must refer the proposed tasking to the authorising officer, who should consider whether a separate authorisation is required.

Version:	4.2	Status of document:	Draft
Author:	Response Policy	PIA:	N/A
Issue Date:	20 th December 2013	Review Date:	20 th December 2014
File Name	BFRSD510100x		

 <p>Buckinghamshire & Milton Keynes Fire Authority MAKING YOU SAFER PREVENTING PROTECTING RESPONDING WWW.BUCKSFIRE.GOV.UK</p>	Information Asset Owner:	Chief Operating Officer Directorate
	Protective Marking:	PROTECT
	Page :	9 of 12
Policy Note: 80-001-002		CHIS and Surveillance Policy

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 Proper records must be kept of the authorisation and use of a source.

14.2 The Regulation of Investigatory Powers (Source Records) Regulations 2000 (SI2000/2725) 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

Version:	4.2	Status of document:	Draft
Author:	Response Policy	PIA:	N/A
Issue Date:	20 th December 2013	Review Date:	20 th December 2014
File Name	BFRSD510100x		

 <p>Buckinghamshire & Milton Keynes Fire Authority MAKING YOU SAFER PREVENTING PROTECTING RESPONDING WWW.BUCKSFIRE.GOV.UK</p>	Information Asset Owner:	Chief Operating Officer Directorate
	Protective Marking:	PROTECT
	Page :	10 of 12
Policy Note: 80-001-002		CHIS and Surveillance Policy

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 Home Office 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. 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.

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

Version:	4.2	Status of document:	Draft
Author:	Response Policy	PIA:	N/A
Issue Date:	20 th December 2013	Review Date:	20 th December 2014
File Name	BFRSD510100x		


 <p>Buckinghamshire & Milton Keynes Fire Authority MAKING YOU SAFER PREVENTING PROTECTING RESPONDING WWW.BUCKSFIRE.GOV.UK</p>	Information Asset Owner:	Chief Operating Officer Directorate
	Protective Marking:	PROTECT
	Page :	11 of 12
Policy Note: 80-001-002		CHIS and Surveillance Policy

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 himself 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 should also abide by the Home Office 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 (SI2000/2793) 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

Version:	4.2	Status of document:	Draft
Author:	Response Policy	PIA:	N/A
Issue Date:	20 th December 2013	Review Date:	20 th December 2014
File Name	BFRSD510100x		

 <p>Buckinghamshire & Milton Keynes Fire Authority MAKING YOU SAFER PREVENTING PROTECTING RESPONDING WWW.BUCKSFIRE.GOV.UK</p>	Information Asset Owner:	Chief Operating Officer Directorate
	Protective Marking:	PROTECT
	Page :	12 of 12
Policy Note: 80-001-002		CHIS and Surveillance Policy

duration of such an authorisation will be only one month, rather than twelve months.

16. Annual review

16.1 In addition, elected members of a local authority should review the authority's use of the 2000 Act and set the policy at least once a year. They should also consider internal reports on use of the 2000 Act on at least a quarterly basis to ensure that it 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.

DRAFT

Version:	4.2	Status of document:	Draft
Author:	Response Policy	PIA:	N/A
Issue Date:	20 th December 2013	Review Date:	20 th December 2014
File Name	BFRSD510100x		