FOLKESTONE & HYTHE DISTRICT COUNCIL

RIPA Policy and Procedures

Issue 14

Assistant Director – Governance, Law and Regulatory Services
Folkestone & Hythe District Council
The Civic Centre
Castle Hill Ave
Folkestone
Kent CT20 2QY

Approved CMT XXXX

Contents

1. Introduction

This Corporate Policy & Procedures Document is based upon the requirements of the Regulation of Investigatory Powers Act 2000 (RIPA) and the Home Office's Code of Practices on Covert Surveillance and Property Interference and Covert Human Intelligence Sources. Covert Surveillance should be used only rarely and in exceptional circumstances. Copies of the Home Office's Codes of Practice are available on its website.

The website should be consulted regularly to ensure that the correct versions of the Codes of Practice are being used.

RIPA and this document are important for the effective and efficient operation of the Council's actions with regard to Covert Surveillance and Covert Human Intelligence Sources. The RIPA Monitoring Officer will therefore keep this document under annual review.

The RIPA Monitoring Officer is responsible for keeping the RIPA forms up to date and for checking the Home Office website and Codes of Practice. The RIPA Monitoring Officer will also be responsible for submitting a report on a three monthly basis to Cabinet on Council's use of RIPA if the Council has used RIPA during the previous three months. The RIPA monitoring officer is also responsible for submitting an annual report to Cabinet on this policy and, if relevant the Council's use of RIPA.

Authorising Officers must bring any suggestions for continuous improvement of this document to the attention of the RIPA Monitoring Officer at the earliest possible opportunity. If any of the Home Office Codes of Practice change, this document will be amended accordingly.

2. Policy Statement

The Council takes its statutory responsibilities seriously and will, at all times, act in accordance with the law and take necessary and proportionate action in these types of matters. In that regard, the Corporate Management Team is duly authorised by the Council to keep this document up to date and to amend, delete, add or substitute relevant provisions as necessary. The Cabinet will if the Council has used RIPA receive the RIPA Monitoring Officer's report every three months. The report will set out the surveillance carried out (though without revealing details of specific operations) and, if appropriate, reporting alterations to this policy. An annual report will be submitted to Cabinet on this policy setting out any alterations since the last report.

It is the policy of the Council that where RIPA applies (see below) surveillance should only be carried out in accordance with this policy.

Where RIPA does not apply, surveillance may properly be carried out provided that the appropriate rules and procedures are followed. For example surveillance connected with an employment issue will have to be carried out in accordance with the Data Protection Act 1998 and the various relevant HR policies. The Council has also adopted a non-RIPA authorisation policy which officers must follow for surveillance which falls outside of RIPA. Advice on non–RIPA surveillance should be sought from Legal Services or HR as appropriate.

3. Roles and Responsibilities of Corporate Directors, Heads of Service, Senior Authorising Officers, Authorising Officers, Senior Responsible Officer and the RIPA Monitoring Officer

This document replaces the previous policy document approved in 2018. It is essential that Corporate Directors, Heads of Service and Authorising Officers take personal responsibility for the effective and efficient operation of this document and the implementation of RIPA in their departments.

The types of surveillance are set out in greater detail below. Directed Surveillance, Intrusive Surveillance and Covert Human Intelligence Sources are described here to aid understanding of the various roles and responsibilities.

Directed Surveillance

Directed Surveillance is surveillance which:

- is covert, but not Intrusive Surveillance;
- is conducted for the purposes of a specific investigation or operation;
- is likely to result in the obtaining of private information about a person (whether or not one specifically identified for the purposes of the investigation or operation);
- is conducted otherwise than by way of an immediate response to events or circumstances the nature of which is such that it would not be reasonably practicable to seek authorisation under the Act.

Intrusive Surveillance

This is when surveillance:

- is covert;
- relates to residential premises and/or private vehicles; and
- involves the presence of a person **in the premises or in the vehicle** or is carried out by a surveillance device **in** the premises/vehicle. Surveillance equipment mounted outside the premises will not be intrusive unless the device consistently provides information of the same quality and detail as might be expected if they were in the premises/vehicle.

Directed Surveillance that is carried out in relation to anything taking place on so much of any premises mentioned below as is, at any time during the surveillance, used for the purpose of legal consultations is also Intrusive Surveillance.

The premises referred to above are:

(a) Any place in which persons who are serving sentences of imprisonment or detention, remanded in custody or committed in custody for trial or sentence may be detained;
(b) Any place in which persons may be detained under paragraph 16(1), (1A) or (2) of Schedule 2 or paragraph 2(2) or (3) of Schedule 3 to the Immigration Act 1971 or section 36(1) of the UK Border Act 2007;
(c) Police stations;
(d) Hospitals where high security psychiatric services are provided;
(e) The place of business of any professional legal adviser;
(f) Any place used for the sittings and business of any court, tribunal, inquest or

inquiry;

(g) Residential accommodation includes rented properties and hotel bedrooms but does not include communal areas of flats unless the area is known to be used by the homeless as a place of abode, hotel reception areas or dining rooms or a front garden readily visible to the public

The Council cannot use RIPA to authorise Intrusive Surveillance.

Covert Human Intelligence Source (CHIS)

A CHIS is someone who establishes or maintains a personal or other relationship for the covert purpose of using the relationship to obtain information.

Roles

Authorising Officer

An Authorising Officer is a person who considers whether or not to grant an application to use Directed Surveillance. He/she must believe the activities to be authorised are necessary for the purposes of preventing or detecting crime and that they are proportionate to what is sought to be achieved by carrying them out.
An Authorising Officer may not, except in case of urgency, consider an application to use Directed Surveillance if the Applying Officer is an officer in his/her service area or the Authorising Officer has direct involvement with the operation.

Senior Authorising Officer

A Senior Authorising Officer is a person responsible for considering whether or not to grant an authorisation where confidential information is likely to be obtained or for use of a CHIS.

Senior Responsible Officer

The Senior Responsible Officer oversees the competence of Authorising Officers and the processes in use in the Council. The Senior Responsible Officer is not an Authorising Officer as it would be inappropriate to oversee his / her own authorisations. Specifically the Senior Responsible Officer will be responsible for:

- The integrity of the processes to authorise Covert Surveillance;
- Compliance with the statutory provisions and codes of conduct;
- Training or arranging training for Authorising Officers;
- Ensuring officers generally understand provisions relating to Covert Surveillance and Covert Human Intelligence Sources.
- Engagement with the Commissioners and inspectors when they conduct their inspections; and
- Overseeing the implementation of any action plans following an inspection.

RIPA Monitoring Officer

The RIPA Monitoring Officer has:

- The duty to maintain the list of Authorising Officers;
- The power to suspend from the list of Authorising Officers any Authorising Officer who does not follow the procedure or who does not attend training sessions; and
- The power to cancel any authorisation that is manifestly wrong.

Responsibilities

Heads of Service are responsible for ensuring their relevant members of staff are suitably trained as 'Applying Officers' so as to avoid common mistakes appearing on forms for RIPA authorisations.

Heads of Service will also ensure that staff who report to them follow this Corporate Policy & Procedures Document and do not undertake or carry out any form of surveillance governed by RIPA without first obtaining the relevant authorisations in compliance with this document. Wilful failure to follow this policy will constitute gross misconduct under the Council's HR policies.

Corporate Directors, Heads of Service, Senior Authorising Officers and 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 a Head of Service permit an application to be made unless, and until s/he is satisfied the health and safety of Council employees/agents are suitably addressed and/or risks minimised, so far as is possible, and proportionate to/with the surveillance being proposed. It is the responsibility of the Applying Officer (i.e. the person who applies to the Authorising Officer to use the Council's RIPA powers) to carry out any risk assessment and complete a written risk assessment if necessary. **If a Head of Service is in any doubt s/he should obtain prior guidance on the same from a Corporate Director, the Head of Paid Service, the Council's Health & Safety Officer or the RIPA Monitoring Officer.**

Authorising Officers must acquaint themselves with the relevant Codes of Practice issued by the Home Office regarding RIPA. Any failure to comply exposes the Council to unnecessary legal risks and criticism from the Investigatory Powers Commissioner's Office. All stages of the process (application, review, renewal and cancellation) must be promptly dealt with.

Coming across **confidential information** during surveillance must be given prior thought before any applications are made or authorised, as failure to do so may invalidate the admissibility of any evidence obtained. Furthermore, thought must be given before any forms are signed to the retention and disposal of any material obtained under a RIPA authorisation. Where confidential information is likely to be obtained through Covert Surveillance, the application must be authorised by a Senior Authorising Officer.

The Authorising Officer must ensure proper regard has been given to **necessity and proportionality** before any applications are authorised. 'Stock phrases' or cut and paste narrative must be avoided at all times as the use of the same may suggest that insufficient detail had been given to the particular circumstances of any person likely to be the subject of the claim. Any **equipment** to be used in any approved surveillance must also be properly controlled, recorded and maintained for audit purposes.

Authorising Officers must ensure that reviews are conducted in a timely manner (best practice for Directed Surveillance is that a review should be carried out no more than 4 weeks after the grant of authorisation) and that cancellations and renewals are effected before the authorisation ceases to have effect.

The RIPA Monitoring Officer shall have responsibility for maintaining, updating and enforcing this Policy. He/she shall also be responsible for the provision of adequate training to Authorising Officers and Applying Officers and for ensuring that no authorisations shall be granted unless the Authorising Officer has received such training.

The RIPA Monitoring Officer shall also ensure that adequate records are maintained in accordance with the relevant and current Code of Practice and also to check that reviews are conducted in a timely manner and that cancellations and renewals are effected before the authorisation ceases to have effect.

The RIPA Monitoring Officer's contact details are set out in Appendix 1 of this Policy.

4. RIPA – General Information

The Human Rights Act 1998 (which brought much of the European Convention on Human Rights and Fundamental Freedom 1950 into UK domestic law) requires the Council, and organisations working on its behalf, pursuant to Article 8 of the European Convention, to respect the private and family life of citizens, his home and his correspondence.

The European Convention did not, however, make this an absolute right, but a qualified right. Accordingly, in certain circumstances, the Council **may** interfere in the citizen's right mentioned above, **if** such interference is:

(a) **In accordance with the law;**
(b) **Necessary** (as defined in this document); **and**
(c) **Proportionate** (as defined in this document).

RIPA provides a statutory mechanism (i.e. in accordance with the law) for authorising **Covert Surveillance** and the use of a **CHIS** e.g. undercover agents. It now also permits public authorities to compel telecommunications and postal companies to obtain and release communications data to themselves in certain circumstances. It works to ensure that **any** interference with an individual's right under Article 8 of the European Convention is **necessary** and **proportionate**. In doing so, RIPA seeks to ensure both the public interest and the human rights of individuals are suitably balanced.

Directly employed Council staff and external agencies working for the Council are covered by the Act for the time they are working for the Council. All external agencies must therefore comply with RIPA and the work carried out by agencies on the Council's behalf must be properly authorised by one of the **Council's Authorising Officers.** It is the responsibility of the Contracts Manger to ensure that external agencies comply with this policy. Authorising Officers are those shown in **Appendix 1** to this document.
If the correct procedures are **not** followed, the courts may disallow evidence, a complaint of maladministration could be made to the Ombudsman, and/or the Council could be ordered to pay compensation. Such action would not, of course, promote the good reputation of the Council and will, undoubtedly, be the subject of adverse press and media interest. In addition wilful failure to follow this policy could constitute gross misconduct under the Council's HR policies. **It is essential, therefore, that all involved with RIPA comply with this document and any further guidance that may be issued.**

Flowcharts of the procedures to be followed appear at **Appendix 2** for Directed Surveillance and for CHIS.

5. When is RIPA authorisation available?

RIPA authorisation is only appropriate for surveillance which relates to the "core functions" of the Council and is for the purpose of preventing or detecting crime.

The core functions of the Council are defined as its "specific public functions" as opposed to its "ordinary functions." The ordinary functions are those functions which any public authority carries out e.g. employment of staff or entering into contractual agreements.

Surveillance whether overt or covert related to ordinary functions is not governed by RIPA and RIPA does not prohibit such activity. The Council has adopted a policy covering the authorisation of surveillance which is not covered by RIPA. The policy can be found here. Advice on such surveillance should be sought from Legal Services and HR as appropriate.

6. What RIPA does and does not do:

RIPA does:

- Compel disclosure of communications data from telecom and postal service providers;
- Permit the Council to obtain communications records from communications service providers.

RIPA does not:

- Make unlawful conduct, which is otherwise lawful.
- 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 the Act. For example, 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 Applying Officer is in any doubt, s/he should ask the RIPA Monitoring Officer BEFORE any Directed Surveillance and/or CHIS is authorised, renewed, cancelled or rejected.

7. Types of Surveillance

'Surveillance' includes:

- Monitoring, observing, listening to persons, watching or following their movements, listening to their conversations and other such activities or communications.
- Recording anything mentioned above in the course of authorised surveillance.
- Surveillance, by or with, the assistance of appropriate surveillance device(s).

Surveillance can be overt or covert.

Overt Surveillance

Most of the surveillance carried out by the Council will be done overtly; there will be nothing secretive, clandestine or hidden about it. In many cases, officers will be behaving in the same way as a normal member of the public (e.g. in the case of most test purchases), and/or will be going about Council business openly (e.g. a market inspector walking through markets).

Similarly, surveillance will be overt if the subject has been **told** it will happen, for example

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.

Covert Surveillance

Covert Surveillance is carried out in a manner calculated to ensure that the person subject to the surveillance is unaware of it taking place (section 26(9) (a) of RIPA). Generally Covert Surveillance cannot be used if there is reasonably available an overt means of finding out the information desired. However if those overt means might seriously undermine the conduct of any investigation or put innocent persons at risk then Covert Surveillance can be used.

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

Directed Surveillance

Directed Surveillance is surveillance which:

- is covert, but not Intrusive Surveillance;
- is conducted for the purposes of a specific investigation or operation;
- is likely to result in the obtaining of private information about a person (whether or not one specifically identified for the purposes of the investigation or operation);
- is conducted otherwise than by way of an immediate response to events or circumstances the nature of which is such that it would not be reasonably practicable to seek authorisation under the Act

Private Information in relation to a person includes any information relating to his private or family life. Private information is generally taken to include any aspect of a person's private or personal relationship with others including family and professional or business relationships. 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 s/he comes into contact or associates with.

To take an example although overt town centre CCTV cameras do not normally require authorisation, if the camera(s) are to be directed for a specific purpose to observe particular individual(s), 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 lives of others.

Social media

Social media can provide useful information as part of an investigation. However, Council Officers must consider if a RIPA authorisation is required if they are accessing social media for this purpose before undertaking any monitoring of a site.

Whilst initial research of social media to establish a fact or collaborate an intelligence picture is unlikely to require an authorisation for Directed Surveillance repeat viewing of 'open

source' sites may constitute Directed Surveillance on a case by case basis and this should be borne in mind e.g. if someone is being monitored through, for example, their Facebook profile for a period of time and a record of the information is kept for later analysis, this is likely to require a RIPA authorisation for Directed Surveillance. The key consideration is whether there is a repeated and systematic collection of personal information.

In addition Council officers must be aware that the fact that digital investigation is routine or easy to conduct does not reduce the need for authorisation. Care must be taken to understand how the social networking site being used works. Authorising Officers must not assume that one service provider is the same as another or that the services provided by a single provider are the same. Whilst it is the responsibility of an individual to set privacy settings to protect unsolicited access to private information and even though data may be deemed published and no longer under the control of the author, it is unwise to regard it as 'open source' or publicly available.

The author has a reasonable expectation of privacy if access controls are applied. In some cases, data may be deemed private communication still in transmission (instant messages for example). Where privacy settings are available but not applied the data may be considered 'open source' and an authorisation is not usually required.

However, repeat viewing of 'open source' sites may constitute Directed Surveillance on a case by case basis and this should be borne in mind e.g. if someone is being monitored through, for example, their Facebook profile for a period of time and a record of the information is kept for later analysis, this is likely to require a RIPA authorisation for Directed Surveillance.

If it is necessary and proportionate for the Council to covertly breach access controls, an authorisation for Directed Surveillance is required. An authorisation for the use and conduct of a CHIS is necessary if a relationship is established or maintained by a Council Officer or by a person acting on the Council's behalf (i.e. the activity is more than mere reading of the site's content). It is not unlawful for a Council Officer to set up a false identity, but this must not be done for a covert purpose without authorisation. Using photographs of other persons without their permission to support the false identity infringes other laws and such photographs must not be used.

To avoid the potential for inadvertent or inappropriate use of social network sites in investigative and enforcement roles, Council officers should be mindful of the following:

- Do not create a false identity in order to 'befriend' individuals on social networks without authorisation under RIPA;
- When viewing an individual's public profile on a social network, do so only to the minimum degree necessary and proportionate in order to obtain evidence to support or refute an investigation;
- Repeated viewing of open profiles on social networks to gather evidence or to monitor an individual's status must only take place under a RIPA authorisation;
- Be aware that it may not be possible to verify the accuracy of information on social networks and if such information is to be used as evidence, take reasonable steps to ensure its validity.

For the avoidance of doubt, only those Officers designated and certified to be Authorising Officers for the purpose of RIPA can authorise Directed Surveillance IF, AND ONLY IF, the RIPA authorisation procedures detailed in this document are followed. Authorisation for Directed Surveillance can only be granted if it is for the purpose of preventing or detecting crime and the criminal offence is punishable by

at least 6 months' imprisonment or it is an offence under sections 146, 147, 147A of the Licensing Act 2003 or section 7 of the Children and Young Persons Act 1933 (sale of alcohol and tobacco to underage children).

If you are in doubt as to whether or not you can use Directed Surveillance for the crime you are investigating, you should contact Legal Services for advice.

Intrusive Surveillance

This is when surveillance:

- Is covert;
- Relates to residential premises and/or private vehicles; and
- Involves the presence of a person **in the premises or in the vehicle** or is carried out by a surveillance device **in** the premises/vehicle. Surveillance equipment mounted outside the premises will not be intrusive, unless the device consistently provides information of the same quality and detail as might be expected if they were in the premises/vehicle.

Directed Surveillance that is carried out in relation to anything taking place on so much of any premises mentioned below as is, at any time during the surveillance, used for the purpose of legal consultations is also Intrusive Surveillance.

The premises referred to above are:

(a) any place in which persons who are serving sentences of imprisonment or detention, remanded in custody or committed in custody for trial or sentence may be detained;
(b) any place in which persons may be detained under paragraph 16(1), (1A) or (2) of Schedule 2 or paragraph 2(2) or (3) of Schedule 3 to the Immigration Act 1971 or section 36(1) of the UK Border Act 2007;
(c) police stations;
(d) hospitals where high security psychiatric services are provided;
(e) the place of business of any professional legal adviser; and
(f) any place used for the sittings and business of any court, tribunal, inquest or inquiry.

This form of surveillance cannot be authorised under RIPA for the Council. Only the Police and other law enforcement agencies can use RIPA to authorise Intrusive Surveillance. Likewise, the Council has no statutory powers to interfere with private property.

Proportionality

The authorisation will not be proportionate if it is excessive in the overall circumstances of the case. Each action authorised should bring an expected benefit to the investigation or operation and should not be disproportionate or arbitrary. No activity should be considered proportionate if the information which is sought could reasonably be obtained by other less intrusive means.

The following elements of proportionality should therefore be considered:

- balancing the size and scope of the proposed activity against the gravity and extent

of the perceived crime or offence;
- explaining how and why the methods to be adopted will cause the least possible intrusion on the subject and others;
- considering whether the activity is an appropriate use of the legislation and a reasonable way, having considered all reasonable alternatives, of obtaining the necessary result;
- evidencing, as far as reasonably practicable, what other methods had been considered and why they were not implemented.

In other words, this means balancing the intrusiveness of the activity on the target subject and others who might be affected by it against the need for the activity in operational terms. The activity will not be proportionate if it is excessive in the circumstances - each case will be judged and be unique on its merits - or if the information that is sought could be reasonably be obtained by other less intrusive means. **All such activity must be carefully managed to meet the objective in question and must not be arbitrary or unfair.** Extra care should also be taken over any publication of the product of the surveillance.

Put very simply, it means not using a sledgehammer to crack a nut.

As well as being proportionate, the Covert Surveillance must be necessary in all the circumstances.

Examples of different types of Surveillance

Type of Surveillance	**Examples**
Overt	- Police Officer or Parks Warden on patrol - Signposted town centre CCTV cameras (in normal use) Recording - noise coming from outside the premises after the occupier has been warned that this will occur if the noise persists. Most test - purchases (where the officer behaves no differently from a normal member of the public).
Covert but not requiring prior authorisation	- CCTV cameras providing general traffic, crime or public safety information.

Directed must be RIPA authorised	- Officers follow an individual or individuals over a period, to establish whether s/he is working when claiming benefit or off long term sick from employment. - Test purchases where the officer has a hidden camera or other recording device to record information which might include information about the private life of a shop-owner, e.g. where s/he is suspected of running his business in an unlawful manner.
Intrusive or interfering with private property – **Note: The Council cannot use RIPA to authorise this**	- Planting a listening or other electronic device (bug) or camera in a person's home or in/on their private vehicle/person.

Further Information

Further guidance on surveillance can be found in the Home Office Codes of Practice is set out in Appendix 5.

Confidential Information

Special safeguards apply with regard to confidential information relating to confidential personal information, confidential constituent information and confidential journalistic material. The Authorising Officer for Directed Surveillance where confidential information is likely to be obtained or for the use of a CHIS must be a Senior Authorising Officer. Further guidance is available in the Home Office Codes of Practice.

Legal Privilege

Surveillance that is intended to result in knowledge of matters subject to legal privilege CANNOT be authorised. Where surveillance is not intended to result in knowledge of matters subject of legal privilege but acquisition of such matters is likely then the Authorising Officer must consider carefully whether such surveillance is appropriate. In particular such surveillance can only be authorised to prevent or detect serious crime. The Authorising Officer in these circumstances must be a Senior Authorising Officer. Further guidance is available in the Home Office Codes of Practice.

Collateral Intrusion

Before authorising surveillance the Authorising Officer should also take into account the risk of intrusion into the privacy of persons other than those who are directly the subjects of the investigation or operation (collateral intrusion). Measures should be taken, wherever practicable, to avoid or minimise unnecessary intrusion into the lives of those not directly connected with the investigation or operation.

Those carrying out the surveillance should inform the authorising officer if the investigation or operation unexpectedly interferes with the privacy of individuals who are not covered by the authorisation. When the original authorisation may not be sufficient, consideration should

be given to whether the authorisation needs to be amended and re-authorised or a new authorisation is required.

Further guidance is available in the Home Office Codes of Practice.

Retention and Destruction of Products of Surveillance

Where the product of surveillance could be relevant to pending or future criminal or civil proceedings, it should be retained in accordance with established disclosure requirements for a suitable period and subject to review. Authorising Officers must make sure that they have regard to the Code of Practice (2005 edition) made under S23 Criminal Procedure and Investigations Act 1996.

There is nothing in RIPA that prevents material obtained from properly authorised surveillance from being used in other investigations. Authorising Officers must ensure, therefore, that arrangements are in place for the handling, storage and destruction of material obtained through the use of Covert Surveillance. Authorising Officers must also ensure compliance with the appropriate data protection requirements and any relevant codes of practice produced by individual authorities relating to the handling and storage of material.

8. Conduct and Use of a Covert Human Intelligence Source (CHIS)

Who is a CHIS?

A CHIS is someone who establishes or maintains a personal or other relationship for the covert purpose of using the relationship to obtain information.

Members of the public who volunteer information to the Council and those engaged by the Council to carry out test purchases in the ordinary course of business (i.e. they do not develop a relationship with the shop attendant and do not use covert recording devices) are not CHIS and do not require RIPA authorisation.

However there may be instances where an individual, covertly discloses information obtained by the use of such a relationship, or as a consequence of the existence of such a relationship. In such circumstances where a member of the public, though not asked to do so, gives information (or repeated information) about a suspect, then serious consideration should be given to designating the individual as a CHIS, particularly if the Council intends to act upon the information received.

It is possible therefore that a person could become engaged in the conduct of a CHIS without the Council inducing, asking or assisting the person to engage in that conduct. As stated in the Home Office statutory CHIS Code of Practice the tasking of a person should not be used as the sole benchmark in seeking a CHIS authorisation. Attention is specifically drawn to the CHIS Code of Practice. It is recommended that legal advice is sought in any such circumstances.

What must be authorised?

The conduct or use of a CHIS require **prior authorisation**

- **Conduct** of a CHIS = Establishing or maintaining a personal or other relationship with a person for the covert purpose of (or is incidental to) obtaining and passing on information

- **Use** of a CHIS = Actions inducing, asking or assisting a person to act as a CHIS and the decision to use a CHIS in the first place.

The Council can only authorise CHIS under RIPA IF, AND ONLY IF THE procedures, as detailed in this document, are followed. Authorisation for CHIS can only be granted if it is for the purposes of preventing or detecting crime.

Juveniles and Vulnerable Individuals

Special safeguards apply to the use or conduct of juvenile sources (i.e. under 18 year olds). On no occasion can a child under 16 years of age be authorised to give information against his or her parents.

A vulnerable individual is a person who is or may be in need of community care services by reason of mental or other disability, age or illness and who is or may be unable to take care of himself or herself, or unable to protect himself or herself against significant harm or exploitation.

Vulnerable individuals and juveniles will only be authorised to act as a CHIS in very exceptional circumstances and a Senior Authorising Officer MUST give the authorisation for their use.

Test Purchases

Carrying out test purchases will not usually (as highlighted above) require the purchaser to establish a relationship with the supplier with the covert purpose of obtaining information and, therefore, the purchaser will not normally be a CHIS.

Anti-Social Behaviour Activities (e.g. noise, violence, race abuse, etc.)

Persons who complain about anti-social behaviour, and are asked to keep a diary will **not** normally be a **CHIS**, as they are not required to establish or maintain a relationship for a covert purpose. Recording the level of noise (e.g. the decibel level) will not normally capture private information and, therefore, does **not** require authorisation.

Recording sound (with a DAT recorder) on private premises could constitute **Intrusive Surveillance**, unless it is done overtly. For example, it will be possible to record if the noisemaker is warned that this will occur if the level of noise continues. Covert recording of noise nuisance where the intention is to record only excessive noise levels from adjoining premises and the recording device is calibrated to record only excessive noise level is unlikely to require authorisation. This is because the perpetrator would normally be regarded as having forfeited any claim to privacy. Placing a covert stationary or mobile video camera outside a building to record anti-social behaviour on residential estates **will** require prior authorisation.

Use and Management of a CHIS

Particular requirements apply to the management and use of a CHIS. This is particularly important when considering that the CHIS may be putting themselves in some jeopardy by performing as a CHIS. Details of those arrangements are contained within **Appendix 3**.

The Senior Authorising Officer must be satisfied that these arrangements are in place before authorising a request. The overriding duty is to the safety of and duty of care towards the CHIS.

Further Information

Further guidance on CHIS can be found in the Home Office's Codes of Practice on surveillance listed in **Appendix 5.**

9. Acquisition of Communications Data

What is Communications Data?

Communication data means any traffic or any information that is or has been sent by over a telecommunications system or postal system, together with information about the use of the system made by any person.

Procedure

There are powers granted by S22 RIPA in respect of the acquisition of Communications Data from telecommunications and postal companies. These issues are beyond the scope of this document. Where an Authorised Officer considers that such data is required, the advice of the RIPA Monitoring Officer should be sought.

10. Authorisation Procedures

Directed Surveillance and the use of a **CHIS** can only gain the protection under RIPA if properly authorised, and conducted in strict accordance with the terms of the authorisation. **Appendix 2** provides flow charts of processes from application/consideration to recording of information and the storage / retention of data obtained.

Authorising Officers

Forms can only be signed by Authorising Officers who have the necessary authority from the Council. Authorised officers are listed in **Appendix 1**. It is the person that is authorised rather than his/her post. This Appendix will be kept up to date by the RIPA Monitoring Officer and added to as needs require. If it is felt that a post should be removed or added, the RIPA Monitoring Officer will request a resolution from the Cabinet. The RIPA Monitoring Officer is however able to suspend an Authorising Officer from the list as detailed above.

All RIPA authorisations must be for specific investigations only and must be reviewed, renewed or cancelled once the specific surveillance is complete or about to expire. **The authorisations for Directed Surveillance last for 3 months and for CHIS 12 months (1 month for juveniles); however they must also be cancelled as soon as the need for them no longer exists.**

Training Records

Authorising Officers and those making applications will receive training in the issues to take into account. The RIPA Monitoring Officer will keep a record of those receiving training and will work with Human Resources to ensure that regular training is carried out to account for staff turnover, legislative changes etc..

Application Forms

Only the RIPA forms set out in this Document are permitted to be used**. The Authorising Officer and/or the RIPA Monitoring Officer will reject any other forms used.** All forms are available on the Intranet.

'A Forms' (Directed Surveillance) -see Appendix 6

Form A1 **Application** for Authority for Directed Surveillance
Form A2 **Review** of Directed Surveillance Authority
Form A3 **Renewal** of Directed Surveillance Authority
Form A4 **Cancellation** of Directed Surveillance
Form A5 **Judicial approval** for Directed Surveillance

'B Forms' (CHIS) -see Appendix 7

Form B1 **Application** for Authority for Conduct and Use of a CHIS
Form B2 **Review** of Conduct and Use of a CHIS
Form B3 **Renewal** of Conduct and Use of a CHIS
Form B4 **Cancellation** of Conduct and Use of a CHIS
Form B5 **Judicial approval** for the use of a CHIS

Grounds for Authorisation

Directed Surveillance (**A Forms**); the Conduct and Use of the CHIS (**B Forms**) can be authorised by the Council **only on the ground of preventing or detecting crime. NO other grounds are available to local authorities.**

Assessing the Application Form

Before an Authorising Officer signs a Form, **s/he must:**

(a) Be mindful of this Corporate Policy & Procedure Document, the training provided and any other guidance issued, from time to time, by the RIPA Monitoring Officer on such matters;

(b) **Be clear on what is being authorised and make sure that there are no ambiguities in either the application or the authorisation;**

(c) **Ensure that his/her statement as the authorising office is completed spelling out the "5Ws" – who, what, where, when, why and how. In addition the authorising officer must ensure that the proposed operation is both necessary and proportionate;**

(d) Satisfy his/herself that the RIPA authorisation is:
  (i) **In accordance with the law**;
  (ii) **Necessary** in the circumstances of the particular case on the ground mentioned above; **and**
  (iii) **Proportionate** to what it seeks to achieve;

(e) In assessing whether or not the proposed surveillance is necessary, consideration should be given to whether it is necessary to use Covert Surveillance in all the circumstances. Consideration must be given as to whether the information could be obtained by other means;

(f) In assessing whether or not the proposed surveillance is proportionate, consider whether there are any other non-intrusive methods available and, if there are none,

whether the proposed surveillance is no more than necessary to achieve the objective, as the **least intrusive method will be considered proportionate by the courts. Guidance on proportionality is given above;**

(g) Take into account the risk of intrusion into the privacy of persons other than the specified subject of the surveillance (**Collateral Intrusion**) and the Applying Officer's plan to minimise that intrusion. Measures must be taken wherever practicable to avoid or minimise (so far as is possible) collateral intrusion. When considering proportionality the right to privacy of both third parties and the intended subject of the investigation must be considered against the seriousness of the offence and harm likely to be caused;

(h) Allocate a Unique Reference Number (URN) for **each form;**

(i) Set a date for **review** of the authorisation and review on that date using the relevant form. The Authorising Officer should take account of how long authorisations for Directed Surveillance may last for (three months). The review date must be appropriate for the type of surveillance sought. At a review the Authorising Officer should be satisfied that the criteria for granting the authorisation still exists. They may also amend the authorisation;

(j) **Make sure that the expiry date and time are inserted;**

(k) Ensure that any RIPA Departmental Register is duly completed, and that a copy of the RIPA Forms (and any review / renewal / cancellation of the same) is forwarded to the RIPA Monitoring Officer's Central Register, **within 2 working days of the relevant authorisation, review, renewal, cancellation or rejection.** The original should be kept on the departmental register.

(l) If unsure on any matter, obtain advice from the RIPA Monitoring Officer **before** signing any forms.

The authorisation section of the form should be completed in the Authorising Officer's own handwriting and in his/her own words. The Authorising Officer must be prepared to justify his/her authorisation in a court of law and must be able to answer for his/her decision.

Additional Safeguards when Authorising a CHIS

When authorising the conduct or use of a CHIS, the Authorising Officer **must also**:

(m) Be satisfied that the **conduct** and/or **use** of the CHIS is **proportionate** to what is sought to be achieved;
(n) Be satisfied that **appropriate arrangements** are in place for the management and oversight of the CHIS and this must address health and safety issues through a written risk assessment **(see Appendix 3);**
(o) Consider the likely degree of intrusion of all those potentially affected;
(p) Consider any adverse impact on community confidence that may result from the use or conduct or the information obtained;
(q) Ensure **records** contain particulars and are not available except on a need to know basis; and
(r) If unsure on any matter, obtain the advice from the RIPA Monitoring Officer **before** signing any forms.

Judicial Approval

After an Authorising Officer has authorised Directed Surveillance or the Senior Authorising Officer has approved the use of a CHIS, the Council **must** make an application to the magistrates' court for approval of the authorisation. This applies to all authorisations and renewals. The activity permitted by the authorisation **cannot** be carried out until the court has approved the authorisation.

After the Authorising Officer has approved the application, the Applying Officer (or the Authorising Officer in appropriate cases) must complete the first part of the approval form found at Appendix 6 and Appendix 7. Two copies of the approval form, the original authorisation and a copy must be taken to court for the magistrate to consider.

The court will consider:

(a) if the Authorising Officer was at the correct grade; and
(b) whether the activity proposed is necessary and proportionate.

The authorisation and the approval form must be detailed enough for the court to consider the application. Whilst the court may ask the officer attending court to clarify the application, oral evidence is not a substitute for a full and reasoned written application.

The court can either approve or quash the authorisation or renewal. Any application for renewal must take place before the expiry of the authorisation. The Applying Officer must ensure that any application to renew is made in good time so that the Authorising Officer and the court have enough time to consider the application.

The original authorisation must be retained by the Council. A copy of the approval or rejection by the magistrates must be placed on the department's register and a further copy given to the RIPA Monitoring Officer for his central register.

Any officer attending court to obtain judicial approval must be authorised by the Council under section 223 of the Local Government Act 1972 to conduct legal proceedings on the Council's behalf.

Further information about the procedure for obtaining judicial approval can be found at Appendix 8.

Duration

The form **must be reviewed in the time stated, renewed and/or cancelled** once it is no longer needed. The authorisation to carry out/conduct the surveillance lasts for 3 months (from authorisation) for Directed Surveillance, and 12 months (from authorisation) for a CHIS. However, whether the surveillance is carried out/conducted or not, in the relevant period, does not mean the authorisation is 'spent'. In other words, **the forms do not expire.** The forms have to be **reviewed, renewed and/or cancelled** (once they are no longer required).

Authorisations can be renewed in writing before the maximum period in the Authorisation has expired. The Authorising Officer must **consider the matter afresh** including taking into account the benefits of the surveillance to date and any collateral intrusion that has occurred. An Authorisation cannot be renewed after it has expired. In such event, a fresh Authorisation will be necessary.

The renewal will begin on the day when the authorisation would have expired.

11. Working With/Through Other Agencies

When some other agency has been instructed on behalf of the Council to undertake any action under RIPA, this document and the forms in it must be used (as per normal procedure) and the agency advised or kept informed, as necessary, of the various requirements. They must be made aware explicitly what they are authorised to do.

When some other agency (e.g. Police, HM Revenue & Customs, Department for Work and Pensions etc):

(a) Wish to use the Council's resources**,** that agency must use its own RIPA procedures **and**, before any Officer agrees to allow the Council's resources to be used for the other agency's purposes, s/he **must obtain** a copy of that agency's RIPA form for the record (a copy of which must be passed to the RIPA Monitoring Officer for the Central Register) or relevant extracts from the same which are sufficient for the purposes of protecting the Council and the use of its resources;

(b) Wish to use the Council's premises for their own RIPA action and is expressly seeking assistance from the Council, the Officer should normally co-operate with the same unless there are security or other good operational or managerial reasons as to why the Council's premises should not be used for the agency's activities. Suitable insurance or other appropriate indemnities may be sought, if necessary, from the other agency for the Council's co-operation in the agency's RIPA operation. In such cases, however, the Council's own RIPA forms should **not** be used, as the Council is only 'assisting' not being 'involved' in the RIPA activity of the external agency.

If the Police or other agency wish to use Council resources for general surveillance, as opposed to specific RIPA operations, an appropriate letter requesting the proposed use, extent of remit, duration, who will be undertaking the general surveillance and the purpose of it must be obtained from the Police or other agency **before** any Council resources are made available for the proposed use. The appropriate Head of Service will be responsible for agreeing to the proposed use.

Joint operations

Where the Council is conducting an investigation jointly with another agency and that investigation involves Directed Surveillance or use of a CHIS only one authorisation under RIPA is needed. Duplicate authorisations therefore should be avoided. At the start of the joint operation the relevant Head of Service should agree with his/her opposite number in the other agency who the lead body should be. The lead body will be responsible for RIPA authorisations.

If in doubt, please consult with the RIPA Monitoring Officer at the earliest opportunity.

12. Record Management

The Council must keep a detailed record of all Authorisations, Reviews, Renewals, Cancellations and rejections in Departments and **a Central Register of all Authorisation Forms will be maintained and monitored by the RIPA Monitoring Officer.**

Records Maintained in the Department

The Council will retain records for a period of at least three years from the ending of the Authorisation. The Investigatory Power Commissioner's Office (IPCO) can audit/review the Council's policies and procedures and individual Authorisations, Reviews, Renewals, Cancellations and rejections.

Central Register Maintained by the RIPA Monitoring Officer

Authorising Officers must send a copy of any authorisation, cancellation, renewal or review to the RIPA Monitoring Officer within 2 working days of the issue. Whilst the RIPA Monitoring Officer is responsible for oversight and review of the records, the Authorising Officers are responsible for their own records.

13. Reporting Arrangements

A one line report will be provided to Cabinet every three months unless there have been any applications for the use of powers under RIPA in which case a full report will be provided to Cabinet.

14. Concluding Remarks

Where there is an interference with the right to respect for private life and family guaranteed under Article 8 of the European Convention on Human Rights, and where there is no other source of lawful authority for the interference, or if it is held not be necessary or proportionate to the circumstances, the consequences of not obtaining or following the correct authorisation procedure set out in RIPA and this document, may be that the action (and the evidence obtained) will be held to be unlawful by the courts pursuant to Section 6 of the Human Rights Act 1998.

Obtaining an authorisation under RIPA and following this document will ensure therefore, that the action is carried out in accordance with this law and subject to stringent safeguards against abuse of anyone's human rights.

Authorising Officers MUST exercise their minds every time they are asked to consider a form. They must NEVER sign or rubber stamp form(s) without thinking about their own personal and the Council's responsibilities. They should also report refusals to the RIPA Monitoring Officer. The RIPA Monitoring Officer will be able to assess whether the refusals were reasonable and this will also be reported to Cabinet.

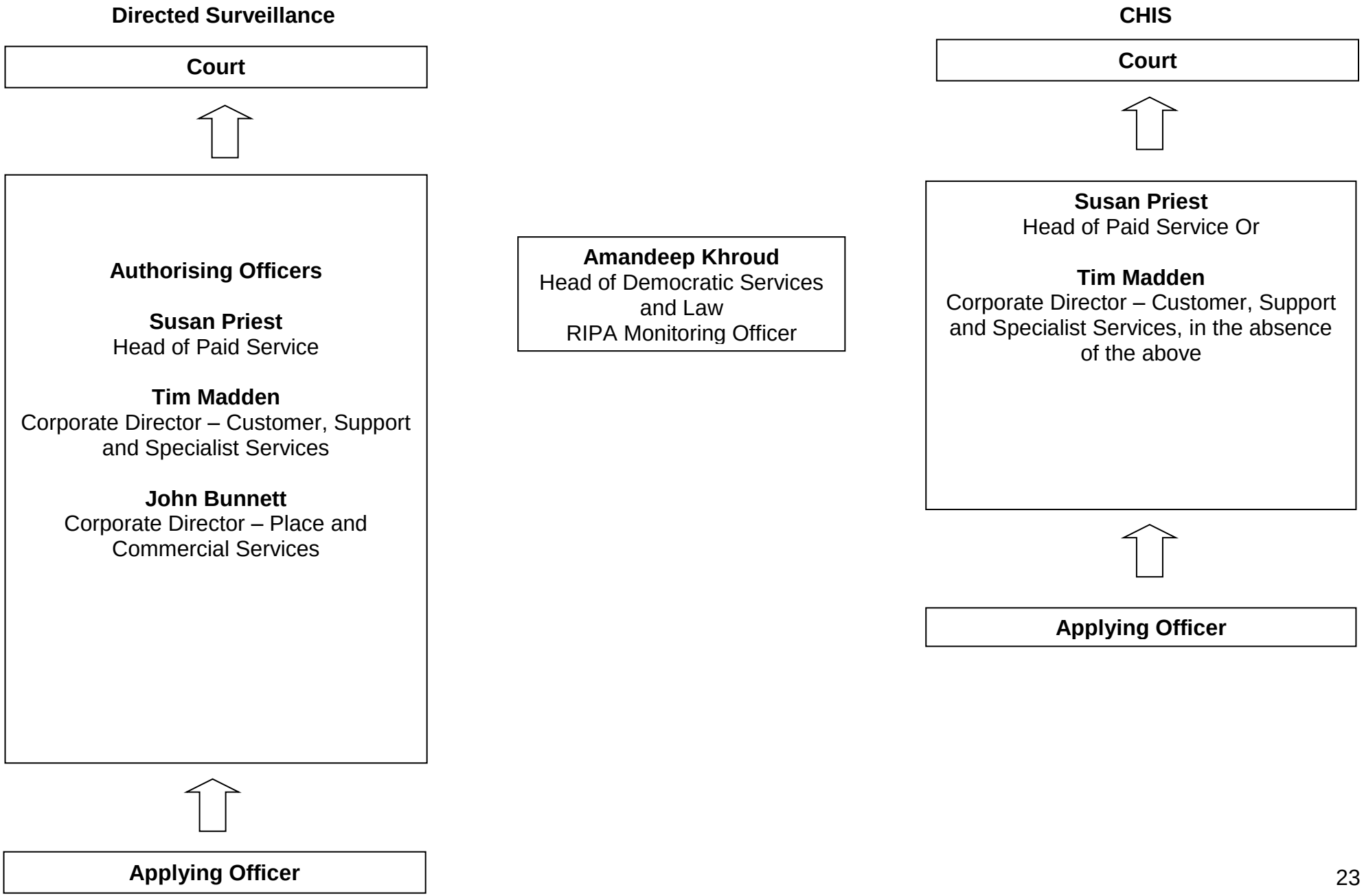
Any boxes not needed on the form(s) must be clearly marked as being 'NOT APPLICABLE', 'N/A' or a line put through the same. Great care must also be taken to ensure accurate information is used and is inserted in the correct boxes. Reason for any refusal of an application must also be kept on the form and the form retained for future audits.

For further advice and assistance on any aspect of RIPA, please contact the Council's RIPA Monitoring Officer; contact details are set out in Appendix 1.

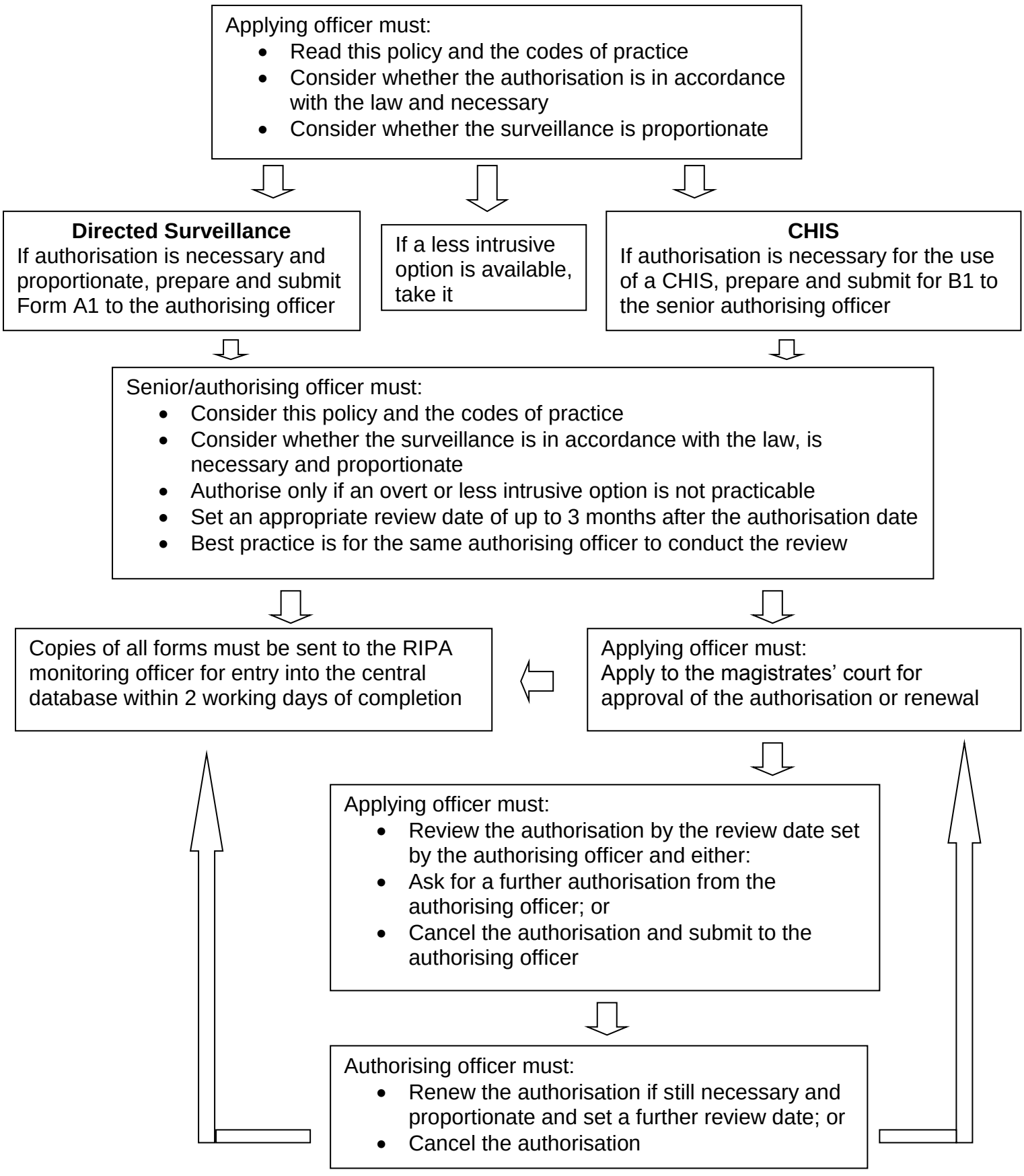
Appendix 1 – List of Senior Authorising Officers, Authorising Officers, Senior Responsible Officer and RIPA Monitoring Officer

Post Title	Current Post Holder	RIPA post	Contact Details
Head of Paid Service	Susan Priest	Senior Authorising Officer / Authorising Officer	Civic Centre, Castle Hill Avenue, Folkestone CT20 2QY 01303 853315 susan.priest@shepway.gov.uk
Corporate Director – Place and Commercial Services	John Bunnett	Authorising Officer	Civic Centre, Castle Hill Avenue, Folkestone CT20 2QY 01303 853263 john.bunnet@ folkestone-hythe.gov.uk
Assistant Director – Governance, Law and Regulatory Services	Amandeep Khroud	RIPA Monitoring Officer Senior Responsible Officer	Civic Centre, Castle Hill Avenue, Folkestone CT20 2QY 01303 853253 amandeep.khroud@folkestone-hythe.gov.uk
Corporate Director – Customer, Support and Specialist Services	Tim Madden	Authorising Officer – Senior Authorising Officer in the absence of the Head of Paid Service	Civic Centre, Castle Hill Avenue, Folkestone CT20 2QY 01303 853371 tim.madden@ folkestone-hythe.gov.uk

RIPA MANAGEMENT STRUCTURE



Appendix 2 – Flow Chart for Directed Surveillance and CHIS



Applying officer – the person who makes a request to use RIPA powers
Authorising officer – the person who considers whether or not to grant an authorisation
Senior authorising officer – the senior person who consider whether or not to grant an authorisation for the use of a CHIS

Appendix 3 – Additional Notes for the Use and Management of a CHIS

Tasking

1 Tasking is the assignment given to the CHIS by the persons defined in sections 29(5) (a) and (b) of RIPA, asking him to obtain information, provide access to information or to otherwise act incidentally, for the benefit of the relevant public authority.

2 Authorisation for the use or conduct of a CHIS must be obtained prior to any tasking where such tasking requires the CHIS to establish or maintain a personal or other relationship for a covert purpose.

3 The person referred to in section 29(5) (a) of the 2000 Act will have day to day responsibility for:

- Dealing with the CHIS on behalf of the Council
- Directing the day to day activities of the CHIS
- Recording the information supplied by the CHIS, and
- Monitoring the CHIS's security and welfare

4 The person referred to in section 29(5) (b) of the 2000 Act will be responsible for the general oversight of the use of the CHIS.

5 The authorisation should not be drawn so narrowly that a separate authorisation is required each time the CHIS is tasked. The authorisation could cover the broad terms of the CHIS's task.

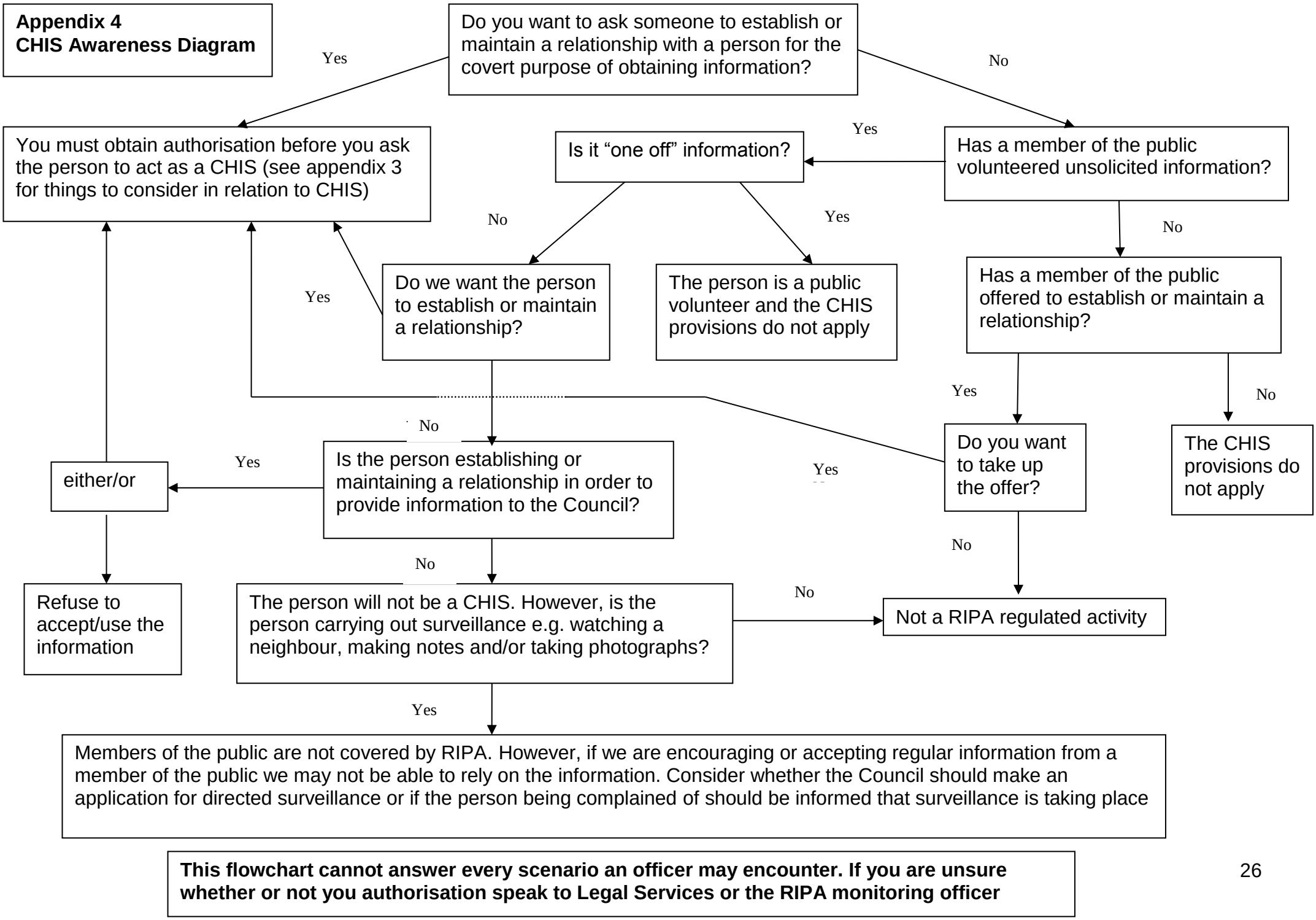
6 The persons mentioned in 3 and 4 above must take great care to ensure that actions are recorded in writing and must also keep the authorisation under review to ensure that it covers what the CHIS is actually doing. During the course of a task, unforeseen events may occur which mean that the authorisation may need to be cancelled and applied for again.

7 The Head of the Paid Service of the Council has the power to appoint officers to act under s29 (5) (a) and (b).

8 In relation to health and safety, before tasking a CHIS, the relevant officers will ensure that a risk assessment is carried out which determines the risk to the CHIS and to others in carrying out the task. The ongoing security and welfare of the CHIS after the task has been completed should also be considered

9 Further advice on good practice is contained with the Code of Practice.

Appendix 4
CHIS Awareness Diagram



This flowchart cannot answer every scenario an officer may encounter. If you are unsure whether or not you authorisation speak to Legal Services or the RIPA monitoring officer

Appendix 5 – Codes of Good Practice

RIPA Codes of Practice can be accessed at:

Codes of Practice

Appendix 6 – Directed Surveillance Forms

Directed surveillance application form

Directed surveillance renewal form

Directed surveillance review form

Directed surveillance cancellation form

Judicial approval form

Appendix 7 – CHIS Forms

Application to authorise a CHIS

CHIS cancellation form

CHIS renewal form

CHIS review form

Judicial approval form

Appendix 8 – Judicial approval protocol

In order to obtain judicial approval for your RIPA authorisation you will need to book an appointment to attend court. You must not turn up to court without an appointment.

To book an appointment, contact the court administration centre on 01304 218600, Option 6. There may be a delay between you making the appointment and attending court so make sure you factor this in when thinking about your timetable and the start date.

Your application may be heard at Folkestone or Canterbury Magistrates' Court. You will generally be asked to attend court at 9.30am before the court starts sitting although you may be given an alternative time to attend.

You will need to take two copies of the approval form with the first part completed and the original authorisation to court as well as a copy. Ensure that you retain the original authorisation and a signed approval form.