FOLKESTONE & HYTHE DISTRICT COUNCIL

Regulation of Investigatory Powers Act 2000 (RIPA) & Investigatory Powers Act 2016

RIPA Policy and Procedures

Issue [17]

Assistant Director (Governance, Law and Regulatory Services)
The Civic Centre
Castle Hill Ave
Folkestone
Kent CT20 2QY

Contents

1. Introduction

This Policy is the framework on which the Council applies the provisions of the Regulation of Investigatory Powers Act 2000 (RIPA) as it relates to covert surveillance. Certain covert powers under RIPA and the Investigatory Powers Act 2016 (IPA) are available to local authorities and can be used in appropriate circumstances in accordance with the requirements of the legislation to support the delivery of their functions. The Investigatory Powers Commissioner's Office (IPCO) oversees the use of covert powers under RIPA by local authorities.

This Policy must be read in conjunction with the Home Office Codes of Practice on Covert Surveillance and Property Interference, the Code of Practice on Covert Human Intelligence Sources and the Code of Practice on Communications Data.

Covert surveillance should be used only when required and it can be justified in an investigation. This will normally be as a last resort. Copies of the Home Office Codes of Practice are available on their website. The Home Office website should be consulted regularly from time to time to ensure that the correct versions of the Codes of Practice are being used.

RIPA and this Policy 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 Policy 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 the Cabinet on the 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. They will also keep the Centrally Recordable Record as required by the Codes of Practice.

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

2. Policy Statement

The Council takes seriously its statutory responsibilities 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 Leadership Team is duly authorised by the Council to keep this Policy 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 covert 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. This Policy covers the use of directed surveillance, intrusive surveillance and the deployment of Covert Human Intelligence

Sources by the Council. These types of surveillance are set out in greater detail in paragraph 7 (Types of Surveillance) below.

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 2018 and the various HR policies. The Council has also adopted a Non-RIPA Authorisation Policy[1] which Officers must follow for covert surveillance which falls outside of RIPA. Advice on non–RIPA surveillance should be sought from legal services or HR as appropriate.

Roles and Responsibilities of Corporate Directors, Assistant Directors, Chief Service Officers, Senior Authorising Officers, Authorising Officers, Senior Responsible Officer and the RIPA Monitoring Officer

This section sets out the various roles and responsibilities in relation to the use of RIPA.

It is essential that Corporate Directors, Assistant Directors, Chief Service Officers and Authorising Officers take personal responsibility for the effective and efficient operation of this Policy and the implementation of RIPA in their departments.

Roles

Authorising Officer

An Authorising Officer is a person who considers whether or not to grant an application to use directed surveillance. They 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. The authorisation is then subject to judicial approval.

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 juvenile CHIS or a vulnerable adult as a CHIS.

Senior Responsible Officer

The Senior Responsible Officer has overall responsibility for the governance and oversight, use and operation of RIPA within the Council, 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. The Senior Responsible Officer should be a member of the Corporate Leadership Team.

Specifically, the Senior Responsible Officer will be responsible for:

- The integrity of the processes in place within the Council for the management of CHIS and directed surveillance;
- Compliance with the statutory provisions and Codes of Practice;
- Training or arranging training for Authorising Officers, together with the RIPA Monitoring Officer;
- Ensuring Officers generally understand provisions relating to covert surveillance and Covert Human Intelligence Sources and communications data;
- Engagement with the IPCO inspectors when they conduct their inspections;
- Overseeing the implementation of any post-inspection action plans approved by the relevant oversight Commissioner;
- Ensuring that all Authorising Officers are of an appropriate standard in light of any recommendations in IPCO inspection reports; and
- Addressing any concerns raised within an IPCO inspection report.

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
- Offer advice to the Authorising Officer where there are deficiencies in the application that have not been able to be resolved with the applying officer.

Responsibilities

Assistant Directors and Chief Service Officers 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.

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

Corporate Directors, Assistant Directors, Chief Service Officers, 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 Assistant Directors or Chief Service Officers permit an application to be made unless, and until, s/he is satisfied that the health and safety of Council employees/agents is 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 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 IPCO. 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 surveillance. 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 and that cancellations and renewals are effected before the authorisation ceases to have effect. Best practice for Directed Surveillance is that a review should be carried out at a frequency specified by the Authorising Officer, based on the activity being authorised but in any event no more than 4 weeks after the grant of authorisation.

The RIPA Monitoring Officer shall have responsibility for maintaining, updating and enforcing this Policy. S/he, in conjunction with the Senior Responsible Officer, 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 Codes 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 Freedoms 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/her home and his/her 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** (see below); **and**
(c) **Proportionate** (see below).

RIPA provides a statutory mechanism (i.e. in accordance with the law) for authorising **covert surveillance** and the use of a **'Covert Human Intelligence Source' (CHIS)** e.g. undercover operatives. 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 RIPA while 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 listed in **Appendix 1** to this Policy.

If the correct procedures are **not** followed, the courts may disallow evidence; a complaint of maladministration could be made to the Investigatory Powers Tribunal (IPT); the Council could be the subject of an adverse report made by the IPCO; and the Human Rights Act 1998 provides a cause of action for damages and/or an injunction against the Council should it be proven that the Council's actions amount to an unwarranted interference with human rights. 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 Policy 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.

Authorisations for both directed surveillance and CHIS are also subject to judicial approval, meaning that the Council must obtain the approval of the Magistrates' Court for any grant or renewal of a RIPA authorisation. The Magistrates' Court will only approve an authorisation where satisfied that the statutory tests have been met, and that the use of the technique is necessary and proportionate. Surveillance cannot commence until this approval has been obtained (see paragraph 10 below for further detail).

Through the application of authorisation procedures and Magistrates' Court approval, RIPA ensures that a balance is maintained between the public interest and the human rights of individuals.

6. What RIPA does and does not do:

RIPA does:

- require prior authorisation of directed surveillance;
- prohibit the Council from carrying out intrusive surveillance;
- compel disclosure of communications data from telecom and postal service providers;
- require authorisation of the conduct and use of a CHIS;
- require safeguards for the conduct and use of a CHIS; and
- permit the Council to obtain communications records from communications service providers.

RIPA does not

- make anything unlawful which is otherwise lawful; or
- 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 <u>overt</u> or <u>covert</u>.

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 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

Intrusive Surveillance

Intrusive surveillance is surveillance which:

- 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.

“Residential premises” means any premises occupied or used, however temporarily, for residential purposes or otherwise as living accommodation. This includes a hotel room or prison accommodation that is occupied or used for residential purposes, but does not include common areas that a person has access to in common with others and in connection with their use of accommodation.

The 2010 Legal Consultations Order also provides that any directed surveillance that is carried out on premises ordinarily used for legal consultations, at a time when they are being so used, is to be treated as intrusive surveillance.

Intrusive 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.

Covert Human Intelligence Source

A Covert Human Intelligence Source ("CHIS") is someone who establishes or maintains a personal or other relationship for the covert purpose of using the relationship to obtain or covertly disclose information (see below)

Private Information in relation to a person includes any information relating to his/her 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. This example does not apply in Folkestone & Hythe as the Council no longer owns nor manages a town / city CCTV system.

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 collate an intelligence picture is unlikely to require an authorisation for directed surveillance, persistent viewing of 'open source' sites may constitute directed surveillance on a case-by-case basis. 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 persistent activity or systematic collection of personal information.

Where it is intended to access a social media or other online account to which the Council has been given access with the consent of the owner, the Council will still need to consider whether the account(s) may contain information about others who have not given their consent. If there is a likelihood of obtaining private information about others, the need for a directed surveillance authorisation should be considered, particularly (though not exclusively) where it is intended to monitor the account going forward.

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
Where information about an individual is placed on a publicly accessible database, for example the telephone directory or Companies House, which is commonly used and known to be accessible to all, they are unlikely to have any reasonable expectation of privacy over the monitoring by public authorities of that information. Individuals who post information on social media networks and other websites whose purpose is to communicate messages to a wide audience are also less likely to hold a reasonable expectation of privacy in relation to that information.

Depending on the nature of the online platform, there may be a reduced expectation of privacy where information relating to a person or group of people is made openly available within the public domain, however in some circumstances privacy implications still apply. This is because the intention when making such information available was not for it to be used for a covert purpose such as investigative activity. This is regardless of whether a user of a website or social media platform has sought to protect such information by restricting its access by activating privacy settings.

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 persona, 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.

In order to determine whether an authorisation should be sought for accessing information on a website as part of a covert investigation or operation, it is necessary to look at the intended purpose and scope of the online activity it is proposed to undertake. Factors that should be considered in establishing whether a directed surveillance authorisation is required include:

- Whether the investigation or research is directed towards an individual or organisation;

- Whether it is likely to result in obtaining private information about a person or group of people;

- Whether it is likely to involve visiting internet sites to build up an intelligence picture or profile;

- Whether the information obtained will be recorded and retained;

- Whether the information is likely to provide an observer with a pattern of lifestyle;

- Whether the information is being combined with other sources of information or intelligence, which amounts to information relating to a person's private life;

- Whether the investigation or research is part of an ongoing piece of work involving repeated viewing of the subject(s);

- Whether it is likely to involve identifying and recording information about third parties, such as friends and family members of the subject of interest, or information posted by third parties, that may include private information and therefore constitute collateral intrusion into the privacy of these third parties.

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 that is necessary and proportionate in order to obtain evidence to support or refute an investigation;
- persistent 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 Policy 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 six months' imprisonment or it is an offence under sections 146, 147, 147A of the Licensing Act 2003,section 7 of the Children and Young Persons Act 1933 (sale of alcohol and tobacco to underage children), section 91 of the Children and Families Act 2014, (purchase of tobacco, nicotine products etc. on behalf of persons under 18) or section 92 of the Children and Families Act 2014 (prohibition of sale of nicotine products to persons under 18).

The Home Office Codes of Practice on covert surveillance and CHIS contain essential guidance in relation to online covert activity and must be consulted.

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 to ensure that no unauthorised online covert activity takes place within the Council.

Necessary

RIPA stipulates that the person granting an authorisation for directed or intrusive surveillance must believe that the activities to be authorised are necessary on one or more statutory grounds. The Regulation of Investigatory Powers (Directed Surveillance and Covert Human Intelligence Sources) (Amendment) Order 2012 has the following effects:

Local authorities in England and Wales can only authorise use of directed surveillance under RIPA to prevent or detect criminal offences that are either punishable, whether on summary conviction or indictment, by a maximum term of at least 6 months' imprisonment or are related to the underage sale of alcohol and tobacco or nicotine inhaling products. The offences relating to the latter are in article 7A of the 2010 RIPA Order.

Local authorities cannot authorise directed surveillance for the purpose of preventing disorder unless this involves a criminal offence(s) punishable (whether on summary conviction or indictment) by a maximum term of at least 6 months' imprisonment.

Proportionality

The authorised conduct will not be proportionate if it is excessive in the overall circumstances of the case. Each authorised action 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 harm;
- 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 subject of the covert activity 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 unique and will be judged on its merits - or if the information that is sought could 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 Environmental Enforcement Officer 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 surveillance (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 surveillance 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.

Further Information

Further guidance on surveillance which 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 to 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 in a limited number of circumstances and particular safeguard apply. 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 must 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 (2020 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.

Material acquired under RIPA and IPA and RRD (Retain, Review & Destroy)
All material obtained under an authorisation must be reviewed to determine if it needs to be retained or destroyed. Covertly obtained material can be retained if there are 'relevant grounds' for doing so or destroyed if the material acquired is no longer needed.

If an initial decision is made to retain the material, then a rolling three-year review period will be used to consider whether the material should be retained or destroyed.

All covertly obtained must be managed in accordance with the relevant Code of Practice. IPCO have also introduced their Data Assurance Programme, which will form part of all future inspections by them. The purpose of the IPCO Data Assurance Programme applies to data obtained under the Investigatory Powers Act (IPA) 2016 and the Regulation of Investigatory Powers Act (RIPA) 2000 and which is therefore the subject of oversight by IPCO. This programme is intended to promote compliance with the IPA and RIPA and the Codes of Practice, and with other legal obligations including the Data Protection Act (DPA) 2018.

IPCO have set six areas which will be inspected upon and the council will ensure that these are all considered when undertaking covert activity. These are:
1. Review the safeguarding obligations in the relevant Code of Practice for any powers used by your authority.
2. Ensure that internal safeguard policies for retaining, reviewing and disposing of any relevant data are accurate and up-to-date.
3. Ensure that the authorising officer for your authority has a full understanding of any

data pathway used for RIPA or IPA data.
4. Ensure that all data obtained under IPA and RIPA is clearly labelled and stored on a data pathway with a known retention policy.
5. Review the wording of safeguards in any applications to obtain data under IPA and RIPA and ensure that they accurately reflect the retention and disposal processes at your authority.
6. Review whether data obtained under previous authorisations is being retained for longer than is necessary and, if appropriate, consider disposing of retained data.

REPORTING OF RELEVANT ERRORS TO IPCO
The Council must report any Relevant Error to IPCO in accordance with the relevant Code of Practice. All reports should be submitted to Errors@ipco.org.uk

Where any further information or action is required as a result of a Relevant Error report, an IPCO Inspector will make contact with the Council. The Relevant Error will then be assessed to determine whether the circumstances could have a) resulted in serious harm or b) call for any urgent changes to national policy or procedures. If this is the case, an investigation will take place. If not deemed serious, the Relevant Error will be addressed at the next inspection.

Relevant Errors will routinely be examined at each inspection. The Council will be required to provide records and confirmation that any material obtained in consequence of the error that has no connection or relevance to any investigation or operation has been destroyed. The SRO is responsible for oversight of reporting errors to the IPC, and the identification of both the cause(s) of errors and implementation of processes to minimise repetition.

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 or covertly disclose information to the local authority as a result.

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 (i.e. “Tasking” – see Appendix 3 for further detail on the use and management of CHIS). As stated in paragraph 2.27 the Home Office CHIS Code of Practice the tasking of a person should not be used as the sole benchmark in seeking a CHIS authorisation, and it is possible that a person will become engaged in the conduct of a CHIS without a local authority inducing, asking or assisting the person to engage in this conduct. it is recommended that legal advice

is sought in any such circumstances.

What must be authorised?

The conduct or use of a CHIS requires **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.

Most CHIS authorisations will be for both use and conduct. This is because public authorities usually take action in connection with the CHIS, such as tasking the CHIS to undertake covert action, and because the CHIS will be expected to take action in relation to the public authority, such as responding to particular tasking.

Authorisations are also subject to judicial approval and cannot commence until this has been obtained.

Detailed records must be kept relating to each source.

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

Juveniles and Vulnerable Individuals

The Investigatory Powers Commissioner (IPCO) must be informed within seven working days of a CHIS authorisation of a vulnerable adult or a juvenile source.

Children as Juvenile CHIS

It is recognised that children are more likely to be more vulnerable that adults due to their age and level of maturity. As a result, enhanced protections are required to ensure their safety and welfare.

Children should only be authorised to act as CHIS in exceptional circumstances and subject to the enhanced risk assessment process set out in Article 5 of the Regulation of Investigatory Powers (Juveniles) Order 2000. The need to safeguard and promote the best interests of the child is a primary consideration in all such CHIS deployments, both when deciding whether to grant the authorisation and during the conduct of any subsequent operation.

On no occasion can a child under 16 years of age be authorised to give information against their parents or person with parental responsibility.

In accordance with the Code of Practice for Covert Human intelligence Sources will only be used in exceptional circumstances and the Authorising Officer will be the Head of Paid Service and the duration will be four months.

If a decision is made to authorise a juvenile CHIS then when making arrangements for meetings, staff must ensure that an appropriate adult is present at any meetings with a

juvenile CHIS who is under 16 years of age when the meeting takes place. Where the CHIS is 16 or 17 years of age consideration will be given on a case-by-case basis following an assessment of the individual's maturity and intelligence to ascertain whether they understand the nature and implications of the role and risk, to undertake the role of a CHIS without an appropriate adult being present.

The rationale for any decision not to have an appropriate adult present will be documented by the Authorising Officer.

Further guidance can be found in the Code of Practice for CHIS, which must be consulted prior to any application being made.

Vulnerable Adults

Special safeguards apply to the authorisation of a vulnerable adult as a CHIS. A vulnerable adult is a person aged 18 or over who by reason of mental disorder or vulnerability, other disability, age, or illness, is or may be unable to take care of themselves, or unable to protect themselves against significant harm or exploitation. Where it is known or suspected that an adult may be vulnerable, they should only be authorised to act as a CHIS in exceptional circumstances. Vulnerable individuals will only be authorised to act as a CHIS in 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. However, using covert recording devices or CCTV cameras to record what is going on in the shop will require **authorisation** as **directed surveillance.** If required, a combined authorisation can be given for a **CHIS** and also **directed surveillance.**

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 residential 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 where the recording is of decibels only or constitutes non-verbal noise (such as music, machinery or an alarm), or the recording of verbal content which is made at a level that does not exceed that which can be heard from the street outside or adjoining property with the naked ear, are unlikely to constitute either direct or intrusive surveillance. In the latter circumstance, 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 but it should be noted that unless this meets the definition of serious crime then it cannot be authorised under RIPA.

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 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 CHIS listed in **Appendix 5.**

9. Acquisition of Communications Data

Communications Data ('CD') is the 'who', 'when' and 'where' of a communication, but not the 'what' (i.e. the content of what was said or written). Local Authorities are not permitted to intercept the content of any person's communications.

Part 3 of the Investigatory Powers Act 2016 (IPA) replaced part 1 chapter 2 of RIPA in relation to the acquisition of communications data (CD. Under the IPA, local authorities can now also obtain details of in and out call data, and cell site location. This information identifies who a criminal suspect is in communication with and whereabouts the suspect was when they made or received a call, or the location from which they were using an Internet service. This additional data is defined as "events" data.

The threshold for which CD "events" data can be sought has been introduced under the IPA as "applicable crime". Defined in section 86(2A) of the Act this means: an offence for which an adult is capable of being sentenced to one year or more in prison; any offence involving violence, resulting in substantial financial gain or involving conduct by a large group of persons in pursuit of a common goal; any offence committed by a body corporate; any offence which involves the sending of a communication or a breach of privacy; or an offence which involves, as an integral part of it, or the sending of a communication or breach of a person's privacy.

Further guidance can be found in the Code of Practice on Communications Data

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 three months and for CHIS 12 months (four months for a juvenile CHIS); however, they must also be cancelled as soon as the need for them no longer exists.**

Training Records

All Council staff who may be involved in the application, authorisation and management of covert activity will receive refresher training as appropriate in the issues to take into account, including in relation to online covert activity. The RIPA Monitoring Officer will keep a record of those receiving training and will work with Human Resources to ensure that training is carried out as appropriate to account for staff turnover, legislative changes etc. Periodic written tests will be conducted to ensure that the Authorising Officers and Applying Officers retain the knowledge.

The training and testing regime will be documented in sufficient detail to enable assessment of its quality and competence.

Application Forms

Only the RIPA forms set out in this Policy 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**) and the Conduct and Use of the CHIS (**B Forms**) can be authorised by the Council **only on the grounds of preventing or detecting crime. NO other grounds are available to local authorities.**

Assessing the Application Form

Before an Authorising Officer signs a Form, **they must:**

(a) Be mindful of this Policy, 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 Officer 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) Believe that the RIPA authorisation is:
- (i) **In accordance with the law**;
- (ii) **Necessary** in the circumstances of the particular case on the grounds mentioned above; **and**
- (iii) **Proportionate** to what it seeks to achieve;
- (iv) Take into account the risk of collateral intrusion into the private lives of those not the subject of the surveillance;
- (v) Be aware of other activities being undertaken by other public authorities that may impact on the authorisation;
- (vi) Be aware of any particular sensitivities in the community and
- (vii) have regard to the Code of Practice,

(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 for the statutory ground of the prevention and detection of crime or preventing disorder. For Directed Surveillance this must be a serious crime or one of the exemptions for underage sales of alcohol or tobacco/nicotine products.

(f) In assessing whether or not the proposed surveillance is proportionate, consider whether there are any other less intrusive methods available and, if there are none, whether the proposed surveillance is no more than necessary to achieve the objective(s), 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 level of intrusion against the need for the activity in operational terms

Particular consideration should be given in cases where religious, medical, journalistic or legally privileged material may be involved, or where communications between a Member of Parliament and another person on constituency business may be involved.

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

(i) Set a date for **review** of the authorisation and review the authorisation on that date using the relevant form. The Authorising Officer should take account The required duration for authorisations for directed surveillance which is 3 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, if it is required and the authorisation allowed for such flexibility when it was initially granted.

(j) **Make sure that the authorisation 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; and

(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**:

(a) Believe that the **conduct** and/or **use** of the CHIS is **proportionate** to what is sought to be achieved. It should be noted that for CHIS activity there is an additional point that is to be considered when considering granting an authorisation. This additional point is that whether the conduct to be authorised will have any implications for the private and family life of others, and an explanation of why (if relevant) it is nevertheless proportionate to proceed with the operation;
(b) 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**);
(c) Take into account the risk of collateral intrusion intrusion of all those potentially affected;
(d) Be aware of any adverse impact on community confidence that may result from the use or conduct or the information obtained;
(e) Ensure **records** contain particulars and are not available except on a need-to-know basis; and
(f) 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. Local authorities are no longer able to orally authorise the use of RIPA techniques. All authorisations must be made in writing and require approval from a Justice

of the Peace.

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/her 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 three months (from authorisation) for Directed Surveillance, and 12 months (from authorisation) for a CHIS and four months for a juvenile 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 Policy 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) Wishes 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 authorisation 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; or

(b) Wishes 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 Assistant Directors or Chief Service Officers 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

Where there has been an application for the use of powers under RIPA, a report on the use of the powers shall, within three months of the application, 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 to be necessary or proportionate to the circumstances, the consequences of not obtaining or following the correct authorisation procedure set out in RIPA and this Policy, 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 Policy 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.

The case of CHATWANI v NCA prescribes that no boxes should be left blank. Therefore, ALL boxes in the application require a full answer and 'NOT APPLICABLE is not an acceptable answer for any of the questions.

In the authorisation, any boxes that are not required to be completed must be clearly marked as 'NOT APPLICABLE'. For example, the boxes relating to an urgent authorisation, as this cannot be granted by a local authority.

Great care must also be taken to ensure accurate information is used and is inserted in

the correct boxes. Reasons 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.

15. Accessing Communications Data

Definition
The Investigatory Powers Act 2016 (IPA) is the legislation governing the acquisition of Communications Data (CD) by Folkestone & Hythe District Council.

Section 60A of the Act provides for the independent authorisation of communications data requests by the Investigatory Powers Commissioner (IPC).

The National Anti-Fraud Network (NFN) provides the services of a dedicated SPoC for acquisition of CD (among other functions).

The Office for Communications Data Authorisations (OCDA) provides the independent authorisation role on behalf of Investigatory Powers Commissioner. An authorising officer in OCDA can authorise any request, for any purpose requested from Folkestone & Hythe District Council, provided it meets the correct application criteria.

The IPA has introduced new definitions of categories of Communications Data which replace those previously described within RIPA. The new categories are Entity Data and Events Data. The definitions are:

- Entity Data relates to the association between an entity and a telecommunications service or telecommunications system and could provide a description and identification of an entity. Entity Data is considered to be less intrusive than Events Data. It can be obtained for the prevention and detection of crime.
- Events Data is any data which identifies or describes an event, (whether or not by reference to its location) on, in or by means of a telecommunications system where the event consists of one or more entities engaging in a specific activity at a specific time. Event data can only be obtained for the prevention and detection of SERIOUS crime.

Serious Crime is defined as,

- An offence by a person who is not an individual (i.e. a corporate body)
- Violence,
- substantial financial gain,
- a large number of persons in pursuit of a common purpose or
- a person of 18 years with no previous convictions could reasonably be expected to be sentenced to 12 months or more imprisonment.

- An offence which involves, as an integral part of it, the sending of a communication.
- An offence which involves, as an integral part of it, a breach of a person's privacy.
- Internet connection records. – not for local authorities.

Folkestone & Hythe District Council is entitled to acquire entity and events data where criteria apply data except for Internet Connection Records.

Examples of entity data are,

i. Subscriber checks,
ii. Subscribers or account holders account information,
iii. Information about the connection, disconnection, and reconnection of services for the subscriber or account holder,
iv. Information about devices used or available to the subscriber or account holder and,
v. Information about the selection of preferred numbers or discount calls.

Examples of event data are,

i. information tracing the origin or destination of a communication including incoming call records,
ii. Information identifying the location of apparatus when a communication is, has been or may be made or received.
iii. Information identifying the sender or recipient (including copy recipients) from data in or attached to the communication,
iv. Routing information identifying apparatus through which a communication is or has been transmitted.
v. Itemised telephone call records and timings and duration.
vi. Information about amounts of data downloaded and/or uploaded,
vii. Information about services to which the user is allocated or has subscribed to e.g., conference calling, call messaging/waiting/barring.

Accessing Communications Data

Folkestone & Hythe District Council use the National Anti-Fraud Network (NAFN) as the SPOC (Single Point of Contact). Applications are approved by a service manager. The approved application is sent to NAFN who facilitate the process of obtaining authority by OCDA. NAFN notify Folkestone & Hythe District Council of the decision and will liaise with the communications data providers to obtain the material.

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 / Senior Responsible Officer	Civic Centre, Castle Hill Avenue, Folkestone CT20 2QY 01303 853315 susan.priest@folkestone-hythe.gov.uk
Director of Corporate Services	Charlotte Spendley	Authorising Officer/ Senior Authorising Officer in the absence of the Head of Paid Service	Civic Centre, Castle Hill Avenue, Folkestone CT20 2QY 01303 853263 Charlotte.spendley@folkestone-hythe.gov.uk
Assistant Director (Governance, Law and Regulatory Services)	Amandeep Khroud	RIPA Monitoring Officer	Civic Centre, Castle Hill Avenue, Folkestone CT20 2QY 01303 853253 amandeep.khroud@folkestone-hythe.gov.uk
Director of Housing & Operations	Andy Blaszkowicz	Authorising Officer	Civic Centre, Castle Hill Avenue, Folkestone CT20 2QY 01303 853315 andrew.blaszkowicz@folkestone-hythe.gov.uk
Director - Place	Ewan Green	Authorising Officer	Civic Centre, Castle Hill Avenue, Folkestone CT20 2QY Ewan.green@folkestone-hythe.gov.uk

RIPA MANAGEMENT STRUCTURE

Directed Surveillance

Court

Authorising Officers

Susan Priest
Head of Paid Service

Charlotte Spendley
Director of Corporate Services

Andrew Blaszkowicz
Director of Housing & Operations

Ewan Green
Director - Place

Applying Officer

Amandeep Khroud
Assistant Director
(Governance, Law and
Regulatory Services)

CHIS

Court

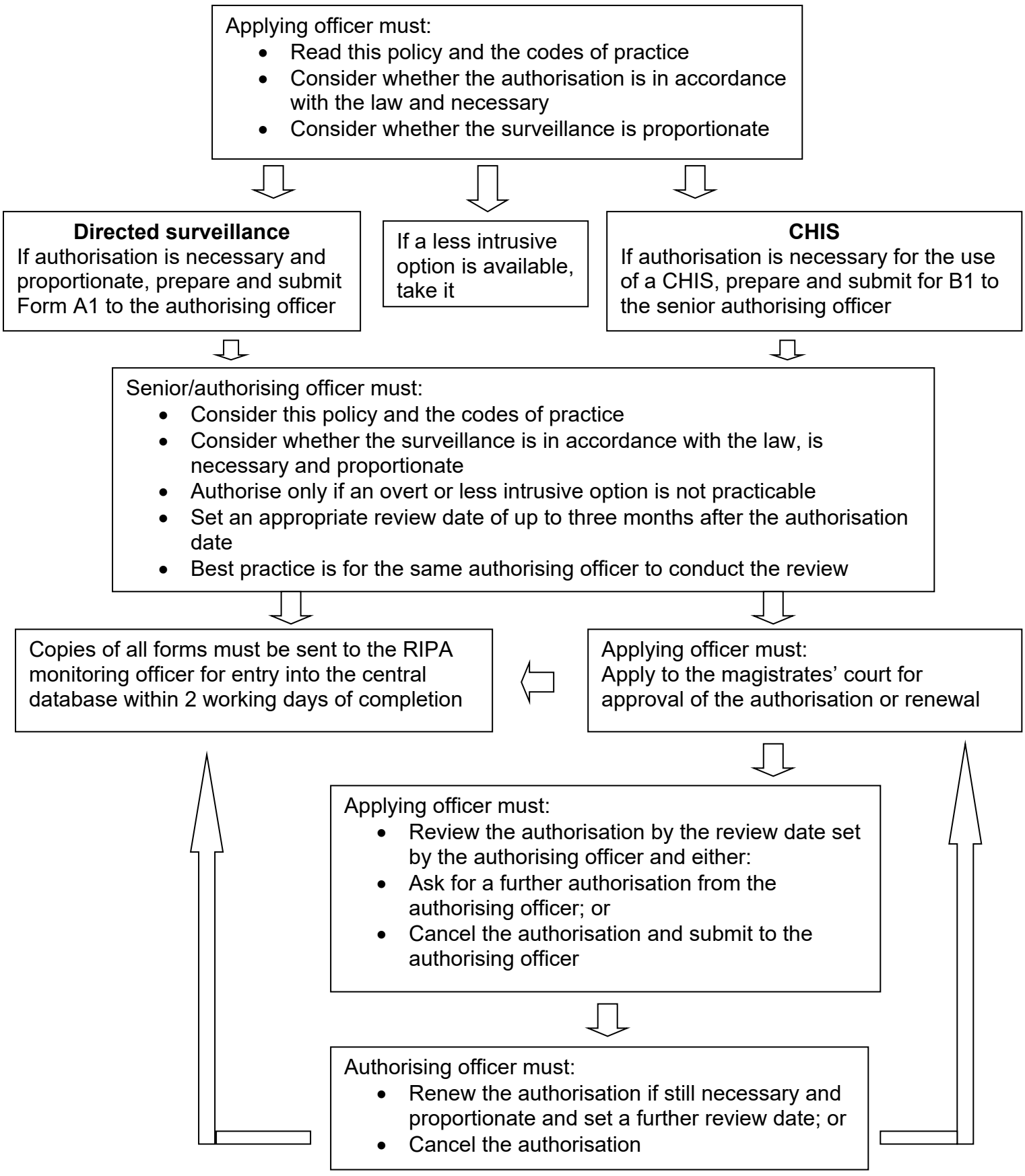
Susan Priest
Head of Paid Service

Or

Charlotte Spendley
Director of Corporate Services

Applying Officer

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 considers 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/her 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 RIPA 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.

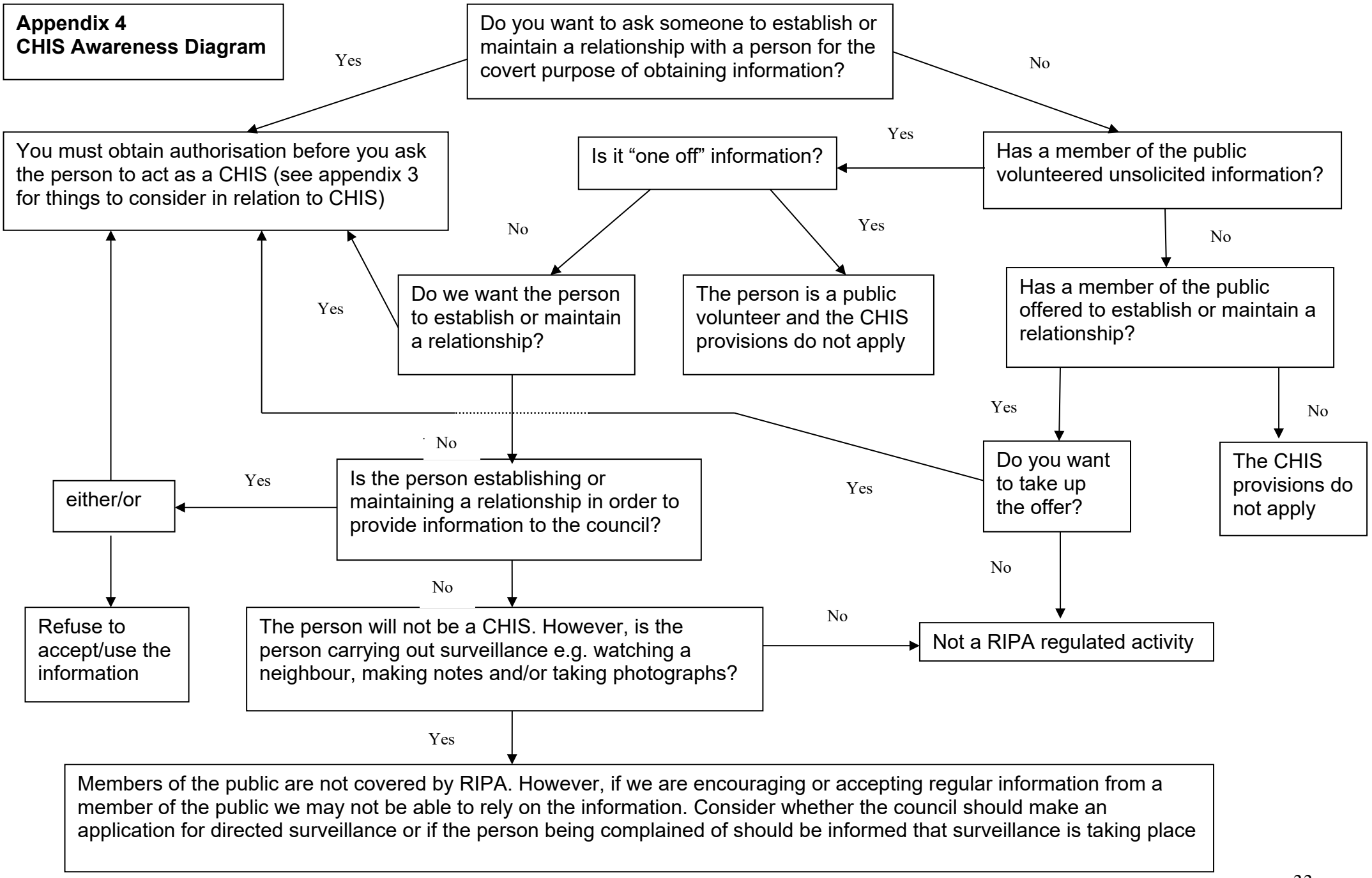
6 The persons mentioned in paragraphs 3 and 4 above must take great care to ensure that actions are recorded in writing and must also keep the authorisation under review to ensure that it covers what the CHIS is actually doing. During the course of a task, unforeseen events may occur which mean that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

7 The Corporate Director – Strategy as Head of Paid Service of the Council has the power to appoint officers to act under s29(5)(a) and (b) of RIPA.

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 within the CHIS 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. This step must not be taken unless an Authorised Officer has first authorised the application.

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.

Appendix 9 – Accessing Communications Data