ANNEXE 1

THANET DISTRICT COUNCIL

REGULATION OF INVESTIGATORY POWERS ACT 2000 ('RIPA')

DRAFT/ POLICY & PROCEDURES GUIDANCE NOTE 2013/14

Version Control

Adopted for Use - *[Cabinet xx June 2013]*

Harvey Patterson
Corporate & Regulatory Services Manager
Thanet District Council
PO Box 9
Cecil Street
Margate CT9 1XZ

Contents

1. Introduction

This Policy & Procedures Guidance Note is based upon the requirements of the Regulation of Investigatory Powers Act 2000 ('RIPA') and the Home Office's Code of Practice on Covert Surveillance and Property Interference and Code of Practice On Covert Human Intelligence Sources.

The guiding principle throughout this Note is that in the discharge of any of the Council's core functions, the use of covert surveillance techniques or the use of a covert human intelligence source ('CHIS') should only ever occur:-

- rarely;
- in exceptional circumstances;
- as a last resort;
- to prevent or detect crime or prevent disorder and for no other purpose whatsoever;

Copies of the Home Office's Codes of Practices are available on their website:

http://security.homeoffice.gov.uk/ripa/publication-search/ripa-cop/.

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

RIPA and this Guidance Note are important for the effective and efficient operation of the Council's actions with regard to authorising covert surveillance operations and the conduct and use of a CHIS. It will therefore be the responsibility of the Senior Responsible Officer ('SRO') to keep this Guidance Note under annual review. Should any of the Home Office Codes of Practice change, he will also be responsible for bringing this to the attention of Authorising Officers and amending this Guidance Note accordingly. The SRO will also be responsible for submitting an information report to the Cabinet on a quarterly basis on the Council's use of RIPA.

The RIPA Co-ordinator is responsible for keeping the Central Register of Authorisations, Reviews, Renewals and Cancellations and it is therefore the responsibility of Authorising Officers to ensure that all the relevant completed forms are promptly passed to the Co-ordinator **within 2 working days**. The RIPA Co-ordinator is also responsible for ensuring that the RIPA forms available on the intranet are up to date.

Authorising Officers are expected to bring any suggestions for continuous improvement of this document to the attention of the Senior Responsible Officer (SRO) at the earliest possible opportunity.

2. Policy Statement

The Council takes its statutory responsibilities seriously and will, at all times, act in accordance with the law and only take necessary and proportionate action in authorising extending and renewing authorisations for the carrying out directed (covert but non-intrusive) surveillance or in the use of a covert human intelligence source.(CHIS) To this end the Senior Management Team ('SMT') is authorised by the Council to approve this Guidance Note and any updates or amendments to it recommended by the SRO or required by legislative amendment or changes in the relevant Codes of Practice. In addition, the Cabinet will receive the SRO's annual

report setting out the surveillance operations carried out in the previous year (without revealing the details of any specific operation) and, if appropriate, reporting any alterations to this Guidance Note approved by SMT.

It is the policy of the Council that where RIPA applies (see below) surveillance should only be carried out strictly in accordance with the Policy and Procedures set out in this Guidance Note.

Where RIPA does not apply surveillance may be carried out provided that the appropriate rules and procedures are followed; for example, covert surveillance connected with an employee must be authorised by the Chief Executive and carried out in compliance with the Data Protection Act 1998. Prior advice on the conduct of surveillance operations not covered by RIPA should be sought from the SRO or the Legal Services Manager.

3. Activities Regulated by RIPA

Four activities are regulated by RIPA - intrusive surveillance, directed surveillance, the conduct or use of a 'covert human intelligence source' ('CHIS') and the obtaining of communications data from telecom and postal services providers including internet service providers. However, the latter activity is outside the scope of this note. The definitions of the three activities which concern this Guidance Note are explained below.

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.

Directed surveillance (see definition below) that is carried out in relation to anything taking place any of the premises mentioned below as is, at any time during the surveillance, being 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.

Important Note - *The Council cannot under any circumstances conduct intrusive surveillance - this is reserved exclusively to the police and security services. Only directed surveillance or the conduct and use of a CHIS may be authorised under RIPA*

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.

Similarly, 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.

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 the SRO or Legal Services Manager for advice.

Covert Human Intelligence Source

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

4. General Information on RIPA

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 and their homes and correspondence.

The European Convention did not, however, make this an absolute right, but a qualified right which the Council may lawfully interfere with provided such interference is:-

(a) **in accordance with the law;**

(b) **necessary** (as defined in this Guidance Note); **and**

(c) **proportionate** (as defined in this Guidance Note).

The Regulation of Investigatory Powers Act 2000 ('RIPA') provides a statutory mechanism (i.e. in accordance with the law) for authorising **directed surveillance, intrusive surveillance** and the use of a **'covert human intelligence source'(CHIS)** (an under cover agent). It now also permits in certain circumstances public authorities to compel telecommunications and postal companies to obtain and release communications data in their possession or control. RIPA seeks to ensure that any interference with an individual's right under Article 8 of the European Convention by intrusive or directed surveillance or by the use of a CHIS is both **necessary** and **proportionate.**

In doing so, RIPA seeks to ensure both the public interest and the human rights of individuals in relation to private and family life and respect for home and correspondence, are suitably balanced.

The Council **cannot** under any circumstances engage in intrusive surveillance, only directed surveillance, and, by definition, directed surveillance is surveillance that is **covert but not intrusive**. Moreover the only basis for the Council authorising directed surveillance or the use or conduct of a CHIS is **for the prevention or detection of a criminal *offence*** *that attracts a sentence of imprisonment of six months or more or a criminal offence that relates to the under age sale of alcohol or tobacco, Consequently, directed surveillance cannot be carried out toprevent disorder unless the conduct under investigation amounted to potential criminal conduct carrying a sentence of imprisonment of six months or more.*

As well as directly employed Council staff, external agencies working for the Council are also covered by the Act for the time they are working for the Council. All external agencies must, therefore, comply with RIPA and the surveillance services carried out by agencies on the Council's behalf must (i) be for the prevention or detection of crime or the prevention of disorder and (ii) be authorised by an Authorising Officer or Senior Authorising Officer. These Officers are identified in **Appendix 1** to this Guidance Note.

Similar principles will apply to joint surveillance operation conducted by Council Officers with another agency such as the police. In setting up the operation agreement should be reached on who is the lead authority for the purposes of obtaining RIPA authorisation. If the Council is in the lead, authorisation should be sought from an Authorising Officer of the Council in accordance with the requirements of this Guidance Note. If, however, the external agency is in the lead they will be responsible for obtaining the necessary RIPA authorisations. However, when agreeing to a joint operation with an external agency in the lead it is the responsibility of the relevant Service Manager to obtain a copy of the relevant authorisation from the agency to ensure that Council staff are lawfully deployed in the operation and pass a copy of that to the RIPA Co-ordinator. Further advice on working with external agencies can be found at **Sections 6 and 10** below.

If proper procedures are not followed, evidence may be inadmissible or disallowed by the courts, a complaint of maladministration could be made to the Ombudsman, and/or the Council could be ordered to pay compensation. Such action would not promote the good reputation of the Council and will, undoubtedly, be the subject of adverse media interest. It is essential, therefore, that all involved with RIPA comply with this Guidance Note. A flowchart of the procedures to be followed is set out in **Appendix 2**.

5. Roles and Responsibilities

A. Specific Roles and Responsibilities

Applying Officer

Any member of staff seeking an authorisation or a renewal authorisation for a surveillance operation or the use of a CHIS

Authorising Officer

A person who determines 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 or preventing disorder and that they are proportionate to what is sought to be achieved by carrying them out.

RIPA Co-ordinator

The RIPA Co-ordinator will be responsible for:

- Maintaining the Central Register of Authorisations, Review, Renewals and Cancellations;
- Keeping the relevant application forms available on the intranet up to date.

Senior Authorising Officer

A person who is responsible for determining whether or not to grant an authorisation for the use or conduct of a CHIS or for directed surveillance where confidential information is likely to be obtained.

Senior Responsible Officer

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;
- Engagement with the Commissioners and Inspectors when they conduct their inspections; and
- Overseeing the implementation of any action plans following an inspection.
- 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

NB The Authorised Officers, Senior Authorised Officers, Senior Responsible Officer and RIPA Co-ordinator are identified in **Appendix 1**

B. General Roles and Responsibilities

It is the responsibility of Service Managers and third tier managers to ensure that relevant members of staff are suitably trained as 'Applying Officers so as to promote understanding of the circumstances which an authorisation, review, renewal or cancellation is required and to promote good practice and accuracy in the completion of the relevant Forms.

Service Managers and third tier managers shall also ensure that staff who report to them follow this Policy and Procedures Guidance Note and do not carry out any form of directed surveillance or seek to recruit or use a CHIS without first obtaining the relevant authorisations in compliance with this Note. Wilful failure to follow this policy will constitute gross misconduct under the Council's HR policies.

Service Managers, third tier managers, 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 and surveillance of any description should not be authorised unless the Authorising Officer is satisfied the health and safety of Council employees or agents are suitably addressed and/or risks minimised, so far as is possible. If an Authorising Officer is in any doubt, s/he should obtain prior guidance from the Council's Health & Safety Advisor. However, it is the responsibility of the Applying Officer or his Service Manager to carry out any risk assessment and complete a written risk assessment if necessary.

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 office of Surveillance Commissioners. All stages of the process (application, review, renewal and cancellation) must be properly dealt with.

Authorising Officers must ensure proper regard has been given to the **necessity and proportionality** of any surveillance authorisation before an application is 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 surveillance. Any **equipment** to be used in any approved surveillance must also be properly controlled, recorded and maintained for audit purposes. Consideration should be given to the use of a plan attached to any authorisation identifying, e.g. the location of the operation and of any equipment to be deployed.

Applying Officers must give prior consideration to the possibility that a surveillance operation could result in the uncovering of confidential or legally privileged information which might invalidate the admissibility of evidence obtained in the operation. If there is any possibility of confidential information being revealed, the application must be authorised by a Senior Authorising Officer who, before granting any application, will consider the retention and disposal of any material likely to be obtained under the authorisation. Further advice on the handling, use, storage and retention of information can be found below at **Section 11** below.

Authorising Officers must also ensure that reviews are conducted in a timely manner, (best practise 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.

Finally, Authorising Officers must also ensure that, when sending copies of any Forms to the RIPA Co-ordinator, the same are sent in a **sealed** envelope marked '**Strictly Private & Confidential'**.

6. Surveillance Guidance

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 or of preventing disorder.

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. **Advice** on such surveillance should be sought from the Corporate & Regulatory Services Manager.

What RIPA does and does not do:

RIPA DOES:

- Require prior authorisation of directed surveillance;
- Prohibit the Council from carrying out intrusive surveillance;
- Require prior authorisation of the conduct and use of a CHIS;
- Require safeguards for the conduct and use of a CHIS;
- 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 an Authorising Officer or any Applying Officer is in any doubt, s/he should seek the advice of the SRO **BEFORE** any directed surveillance and/or the use of a CHIS is authorised, rejected, reviewed, renewed or cancelled.

Types of Surveillance

As mentioned in Section 3 above, this Guidance Note concerns three of the four specific activities regulated by RIPA; intrusive Surveillance, Directed Surveillance and the use of CHIS. However, the Council may not engage in intrusive surveillance

under any circumstances and may only authorise directed surveillance or the conduct or use of a CHIS *for the purpose of preventing or detecting criminal offences that carry a sentence of imprisonment of six month or more or relate to the under-age sale of alcohol ot tobacco*. The definitions of directed surveillance and a CHIS is also set out in **Section 3** above

'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 a premises licence authorising public entertainments 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.

Tests of Necessity and Proportionality

Assuming an Authorising Officer receives an application form from an Applying Officer seeking an authorisation for a directed surveillance operation in relation to a core business activity which demonstrates a clear crime and disorder prevention purpose. What other tests need to be satisfied for the application to be granted? Firstly, the surveillance operation must be **necessary** in all the circumstances and secondly, even if it is necessary, the surveillance operation proposed must be **proportionate**. If both these tests are not met, the application must be rejected.

A covert surveillance operation will not be **necessary** if the information/evidence sought can reasonably be obtained by other less intrusive means, for example by carrying out overt surveillance. Therefore Applying Officers should address this test by describing any other means by which the information could be obtained and the reasons why this not practical - for example, if overt surveillance would alert the suspect and result in the destruction of evidence.

An 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 or if the information that is sought could be reasonably be obtained by other less intrusive means.

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

Examples of different types of Surveillance

Type of Surveillance	**Examples**
Overt – RIPA not engaged	- 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 employments. - 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 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 guidance on surveillance can be found in the Home Office Codes of Practice is set out in **Appendix 4**

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 or for the use of a CHIS where confidential information is likely to be obtained must be a Senior Authorising Officer. Further guidance is available in the Home Office Codes of Practice set out in **Appendix 4.**

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 the 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 and can only be authorised by a Senior Authorising Officer. Further guidance is available in the Home Office Codes of Practice set out in **Appendix 4.**

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 set out in **Appendix 4.**

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. Further advice on Records Management is given at **Section 11** below.

7. CHIS Guidance

Who is a CHIS?

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

RIPA does **not** apply in circumstances where members of the public **volunteer** information to the Council as part of their normal civic duties. However if the member of the public is asked to get further information or if that information that they have covertly gathered is used and could be traced to them consideration must be given to authorising them as a CHIS.

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 a CHIS can only be granted if it is for the purposes of preventing or detecting crime or preventing disorder.

Consult the SRO

Any officer considering using a CHIS must first consult the SRO for advice before taking any action.

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. Similarly, using mobile hidden recording devices or CCTV cameras to record what is

going on in the shop will require **authorisation** as **directed surveillance.** A combined authorisation can be given for a **CHIS** and also **directed surveillance.**

Anti-Social Behaviour Activities (e.g. noise, violence, harassment, racially motivated 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 devise 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**.

A **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 4.**

8. 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 Corporate & Regulatory Services Manager should be sought.

9. Authorisation Procedures

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

Authorising Officers

Applications can only be granted in writing and by by the Authorising Officers listed in **Appendix 1** using the requisite forms - see below. It is the person named in Appendix 1 who is authorised, not the post holder. This Appendix will be kept under review by the SRO and if s/he considers that a post should be removed or added, the SRO will request a resolution from SMT. The SRO 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's for 12 months. However they must also be cancelled as soon as the need for them no longer exists.**

Application Forms

Only the RIPA forms set out in this Document are permitted to be used. The Authorising Office and/or SRO will reject any other form used. All forms are available on TOM (the intranet).

'A' Forms (Directed Surveillance) - see Appendix 5

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 5

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 Conduct and 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 grounds of **preventing or detecting crime or preventing disorder. NO other grounds are available to local authorities.**

Assessing the Application Form

Before an Authorising Officer authorises an application **s/he must: -**

(a) Be mindful of this Policy & Procedure Guidance Note, the training provided and any other guidance issued, from time to time, by the SRO 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 authorising a surveillance operation 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 grounds mentioned in above; **and**

(iii) **proportionate** to what it seeks to achieve.

(e) In assessing whether or not the proposed surveillance is necessary, consider whether in all the circumstances it is necessary to use covert surveillance and what information could be obtained by other means. Further guidance on necessity is given at **Section 6** above

(f) In assessing whether or not the proposed surveillance is proportionate, consider whether there are any other non-intrusive, 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. Further guidance on proportionality is given at Section 6 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) Take into account any Health & Safety Risks arising out of the proposed operation and consider the risk assessment prepared by the Applying Officer.

(i) Allocate a **Unique Reference Numbe**r *(URN) for each form.

(j) 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;

(k) Make sure that the expiry date and time are inserted.

(l) 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 Co-ordinator for entry in the Central Register, **within 2 working days of the relevant authorisation rejection, review, renewal or cancellation.** The original should be kept on the departmental register.

(m) If unsure on any matter, obtain advice from the SRO **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 **Senior** Authorising Officer **must also**: -

(a) Be satisfied that the **conduct** and/or **use** of the CHIS is **proportionate** to what is sought to be achieved;

(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 4);**

(c) Consider the likely degree of intrusion of all those potentially affected;

(d) Consider 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 advice is needed, seek advice from the SRO or the Legal Services Manager **before** taking any actions.

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 5. 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 Co-ordinator 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.

Urgent Authorisations

Urgent authorisations are not often necessary but there are circumstances that may give rise to them**.** In exceptional circumstances, therefore, urgent authorisations may be given orally if the time that would elapse before a written authorisation can be granted would be likely to **endanger life or jeopardise the investigation or operation** for which the authorisation was being given.

It will not be urgent where the need for authorisation has been neglected or is of the Officer's own making. All urgent authorisations must be notified to the RIPA Monitoring Officer within 24 hours of the oral authorisation for the Central Register.

Urgent authorisations last for 72 hours unless cancelled first. They must be recorded in writing on the standard form on the electronic database as soon as practicable and the extra boxes on the form completed to explain why the urgent oral authorisation was necessary.

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 72 hours (from authorisation) for urgent authorisations 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**

Urgent oral authorisation, if not already ratified in a written authorisation, will cease to have effect after 72 hours, beginning with the time when the authorisation was granted.

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 in exceptional circumstances, renewals may be granted orally in urgent cases and last for a period of seventy-two hours.

10. 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, Revenue & Customs etc):-

(a) Wish to use the Council's **resources** (e.g. CCTV surveillance systems), 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 Co-ordinator for entry on the Central Register);

(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 agent'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.

In terms of 2(a), 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 the conduct 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 Service Manager should agree with his/her opposite number in the other agency who the lead authority should be and the lead authority will be responsible for RIPA authorisations. However, if the external agency is the lead authority, the Service **must obtain** a copy of that agency's RIPA authorisation forms for the record a copy of which must be passed to the RIPA Co-ordinator for entry on the Central Register.

If in doubt, please consult with the SRO at the earliest opportunity.

11. Records 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 Co-ordinator.**

Records Maintained in the Department

The Council will retain records for a period of at least three years from the ending of an Authorisation. The Office of the Surveillance Commissioners (OSC) can audit/review the Council's Policy and Procedures Guidance Note and individual Authorisations, Reviews, Renewals, Cancellations and rejections.

Central Register Maintained by the RIPA Co-ordinator

Authorising Officers must send a copy of any authorisation, any cancellation, renewal or review to the RIPA Co-ordinator within 2 working days of the issue. Whilst the Senior Responsible Officer is responsible for oversight and review of the records, the Authorising Officers are responsible for their own records and ensuring that authorisations are reviewed, extended or cancelled as appropriate.

12. Reporting Arrangements

The Cabinet will receive an annual report reviewing the Council's use of covert surveillance techniques in the previous year although no personal data relating to a specific authorisation will be disclosed.

Training Records

Authorising Officers and those making applications will receive training in the issues to take into account. The Senior Responsible 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. Periodic written tests may be conducted to ensure that the Authorising Officers and Applying Officers retain knowledge.

13. 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 SRO and the SRO will assess whether the refusals were reasonable.

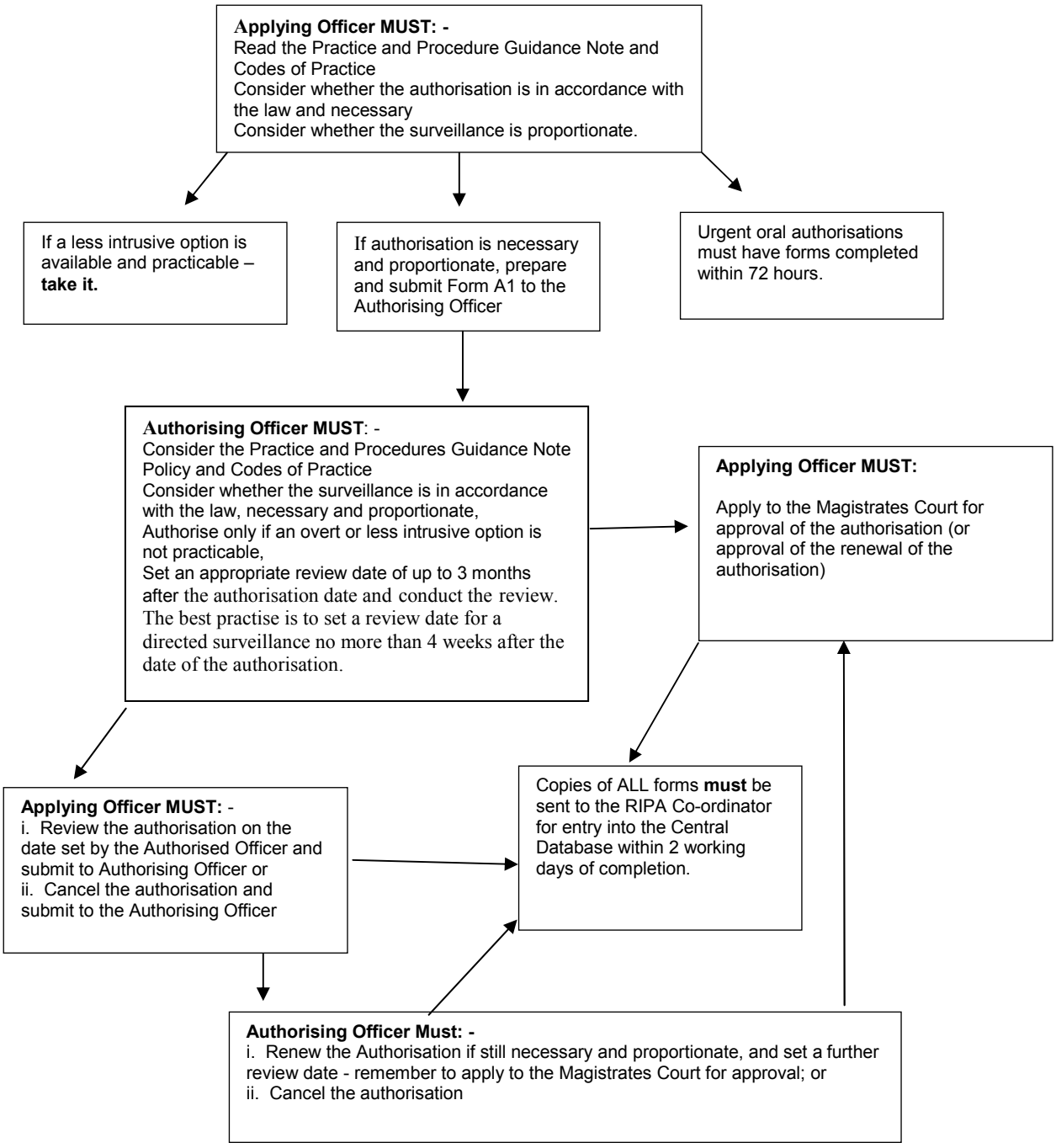
Any boxes not needed on the Form(s) must be clearly marked as being 'NOT APPLICABLE', 'N/A' or a line put through the same. Great care must also be taken to ensure accurate information is used and is inserted in the correct boxes. Reason for any refusal of an application must also be kept on the form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

For further advice and assistance on any aspect of RIPA, please contact the Senior Responsible Officer - contact details are set out in **Appendix 1.**

Appendix 1 – List of Senior Authorising Officers Authorising Officers, Senior Responsible Officer and RIPA Co-ordinator

Post Title	Current Post Holder	RIPA post	Contact Details
Chief Executive	Sue McGonigal	Senior Authorising Officer Authorising Officer	PO Box 9, Cecil Street, Margate, CT9 1XZ 01843 577001 **Sue.McGonigal@Thanet.gov.uk**
Director of Community Services	Madeline Homer	Senior Authorising Officer (in the absence of the Chief Executive) Authorising Officer	PO Box 9, Cecil Street, Margate, CT9 1XZ 01843 577123 **Madeline. Homer@Thanet.gov.uk**
Director of Commercial Services	Mark Seed	Authorising Officer	PO Box 9, Cecil Street, Margate, CT9 1XZ 01843 577742 **Mark.Seed@Thanet.gov.uk**
Corporate & Regulatory Services Manager	Harvey Patterson	Senior Responsible Officer Authorising Officer	PO Box 9, Cecil Street, Margate, CT9 1XZ 01843 577005 **Harvey.Patterson@Thanet.gov.uk**
Financial Services Manager	Sarah Martin	Authorising Officer	PO Box 9, Cecil Street, Margate, CT9 1XZ 01843 577617 **Sarah.Martin@Thanet.gov.uk**
Director of Shared Services – East Kent Services	Donna Read	Authorising Officer	PO Box 9, Cecil Street, Margate, CT9 1XZ 01227 862073 or 07753 980023 **donna.reed@ekservices.org**
Democratic Services & Scrutiny Manager	Glenn Back	RIPA Co-ordinator	PO Box 9, Cecil Street, Margate, CT9 1XZ 01843 577187 **Glenn.Back@Thanet.gov.uk**

Appendix 2 - Flow Chart for Directed Surveillance and CHIS



Terminology:

Applying Officer – The person who makes a request to use RIPA powers to the Authorising Officer

Authorising Officer – The person who considers whether or not to grant an authorisation.

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

Tasking.

1. Tasking is the assignment given to the CHIS by the handler and controller, 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 Chief Executive 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 afte the task has been completed should also be considered.

9. Advice must be sought from another agency/agencies who are experienced in using CHIS's (e.g. the Police) on the procedures and practices to be allowed.

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

Appendix 4 - Codes of Good Practice

RIPA Codes of Practice can be accessed at:

http://security.homeoffice.gov.uk/ripa/publication-search/ripa-cop/

Appendix 5 - Directed Surveillance Forms*

Form A1: **Application** for authorisation to carry out directed surveillance.

Form A2: Application for **Review** of Form A1

Form A3: Application for **Renewa**l of Form A1

Form A4: **Cancellation** of Form A1

Form A5: **Judicial Approval** for Directed Surveillance

* These forms may be downloaded from the Council's intranet.

Appendix 6 - CHIS Forms*

Form B1: **Application** for authorisation to use a CHIS

Form B2: Application for **Review** of Form B1

Form B3: Application for **Renewa**l of Form B1

Form B4: **Cancellation** of Form B1

Form B6: **Judicial Approval** for Use of a CHIS

* These forms may be downloaded from the Council's intranet.