A great place to live, work & play

SCARBOROUGH BOROUGH COUNCIL

REGULATION OF INVESTIGATORY POWERS ACT 2000 (RIPA)

POLICY AND PROCEDURES

20 March 2018

DOCUMENT CONTROL

Author	Carol Rehill
Owner	Regulation and Governance Services
Protective Marking	NOT PROTECTIVELY MARKED
Cabinet Approval Date	
Council Approval Date	
Policy Date/Period	
Policy Review Frequency	Annually

REVIEW HISTORY

Date	Reviewed By	Version	Any Revisions?

REVISION HISTORY (only required where changes made)

Date	Revised By	Version	Description of Revision
20 March 2018	**David Kitson**	0.1	Updated
20 Sept 2018	Petra Jackson	0.2	Updated – to reflect IPCO, delete references to Deputy CE

DOCUMENT REVISION APPROVALS

Version	Approval	Date
	Standards Committee	20 March 2018

CONTENTS

APPENDICES

1. INTRODUCTION AND BACKGROUND

1.1 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. It must be read in conjunction with the statutory codes of practice issued by the Secretary of State and any additional guidance provided by individual Directorates relevant to their respective service areas.

1.2 Article 8 of the Human Rights Act 2000 (HRA) provides the right to respect for private and family life:

'Everyone has the right to respect for his private and family life, his home and his correspondence.'

1.3 Article 8 of the HRA goes on to state:

'There shall be no interference by a public authority with the exercise of this right except such as in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, ***for the prevention of disorder or crime****, for the protection of health or morals, or for the protection of the rights and freedoms of others.'*

1.4 The rights conferred by Article 8 are therefore qualified, meaning that the Council may interfere with these rights providing that such interference is:

- in accordance with the law;
- necessary; and
- proportionate.

1.1 RIPA provides a statutory framework under which the Council may seek authorisation to permit;

- the use of Directed Surveillance;
- the use of Covert Human Intelligence Sources (CHIS); and
- the Acquisition and Disclosure of Communications Data.

1.5 The Council's ability to use RIPA legislation is limited, and in practice only directed surveillance is likely to be relevant, for reasons set out within this Policy.

1.6 Use of a CHIS must never be undertaken without consultation with the Senior Responsible Officer.

1.7 Local Authorities can only authorise the use of directed surveillance on the grounds of;

(a) the prevention or detection of criminal offences (that are either

punishable by a maximum of at least 6 month's imprisonment OR are related to the underage sale of alcohol and tobacco); or

(b) the prevention of disorder that involves at least one criminal offence that is punishable by a maximum of at least 6 month's imprisonment.

1.8 The Council cannot therefore authorise the use of directed surveillance to investigate disorder that does not involve criminal offences, or to investigate low-level offences such as littering, dog fouling or fly-posting.

1.9 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. Authorisation cannot commence until this approval has been obtained.

1.10 Applications to the Magistrates' Court for approval of an Authorisation must be made in accordance with the requirements of the Court.

1.11 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.

1.12 If the RIPA procedures are followed correctly the conduct of an investigation will be deemed lawful for all purposes (section 27 RIPA). This protection extends to criminal and civil proceedings, Employment Tribunal hearings and a complaint to either the Local Government Ombudsman or the Investigatory Powers Tribunal. It therefore provides protection both for the Council and any Officer who may have been involved in an investigation.

1.13 Unauthorised covert surveillance will likely be a breach of a person's right to privacy under Article 8. Even if surveillance without due Authorisation in a particular instance is not illegal, if Authorisation is not obtained, the surveillance carried out will not have the protection that RIPA affords.

1.14 If the correct procedures are not followed;

- The Authorisation will not take effect as it will not be approved by the Magistrates' Court;
- Court proceedings that rely upon the information obtained by surveillance may be undermined;
- A complaint of maladministration may be made to the Ombudsman;
- The Council could be the subject of an adverse Report by the Investigatory Powers Commissioner's Office;

- The HRA provides a cause of action for damages and/or an injunction against the Council should it be proven that the Councils' actions amount to an unwarranted interference with human rights.

1.15 Such action would not promote the good reputation of the Council and will undoubtedly be the subject of adverse press and media interest. It is therefore essential that all involved with RIPA comply with this Document and any further guidance that may be issued from time to time.

1.16 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;
- permit the Council to obtain communications records from Communications Service Providers.

1.17 RIPA does not;

- make unlawful anything that is otherwise lawful;
- impose any new statutory duties;
- prejudice or dis-apply any existing powers available to the Council to obtain information by any means not involving conduct that is governed by RIPA. (For example it does not affect the Council's current powers to obtain information from the DVLA or the Land Registry).

1.18 If the Authorising Officer or any Applicant is in any doubt, they should consult the Senior Responsible Officer BEFORE any directed surveillance and/or CHIS is authorised, renewed, cancelled or rejected.

1.19 The use of the powers conferred by RIPA is subject to scrutiny by the Investigatory Power's Commissioner's Office, which carries out periodic inspections of the Council's practices and procedures. Furthermore, RIPA also provides for the establishment of a Tribunal to determine complaints about the use of RIPA powers. It is therefore essential that surveillance is always carried out in compliance with RIPA, the policies and codes of practice referred to in this document, and any advice or guidance that may be issued from time to time.

2. RIPA MANAGEMENT

2.1 This section sets out the various roles and responsibilities in relation to the use of RIPA. Some of this information is repeated throughout this document, however this is due to the importance in understanding the same.

2.2 Set out at Appendix A is a concise list of roles and the posts to which they are assigned.

2.3 Senior Responsible Officer

2.3.1 The Senior Responsible Officer (SRO) has overall responsibility for the use and operation of RIPA within the Council, and should be a member of the corporate leadership team.

2.3.2 In particular they are responsible for:

(a) the integrity of the process in place within the Council for the management of CHIS and Directed Surveillance;

(b) compliance with the Act and with the Codes;

(c) engagement with the IPCO inspectors when they conduct their inspections, where applicable;

(d) where necessary, oversight of the implementation of post-inspection action plans approved by the relevant oversight Commissioner;

(e) ensuring that all Authorising Officers are of an appropriate standard in light of any recommendations in IPCO inspection reports;

(f) addressing any concerns raised within an IPCO inspection report;

(g) providing advice to Officers regarding potential RIPA applications; and

(h) organising a RIPA training programme (together with the Coordinating Officer).

2.4 Coordinating Officer

2.4.1 The Coordinating Officer (CO) is responsible for:

(a) maintaining the Central Record of Authorisations;

(b) collating original applications/authorisations, reviews, renewals and cancellations;

(c) organising applications for authorisation to the Magistrates' Court;

(d) oversight of submitted RIPA documentation;

(e) the provision of advice to Officers considering the use of RIPA;

(f) the provision of advice to Officers at the stage of authorisation;

(g) organising a RIPA training programme (together with the SRO); and

(h) raising RIPA awareness within the Council.

2.4.2 The Coordinating Officer should not be an Authorising Officer, as this would conflict with the primary responsibility of oversight of RIPA documentation.

2.5 Authorising Officer

2.5.1 Responsibility for authorising the carrying out of directed surveillance or the use of CHIS (both subject to Magistrates Court approval) rests with the Authorising Officer.

2.5.2 Authorising Officers must hold the office of at least Director, Head of Service, Service Manager or equivalent.

2.5.3 Only the Chief Executive and the Council's Monitoring Officer can authorise the use of a juvenile or vulnerable CHIS, or surveillance where confidential information is likely to be acquired, and would only be expected to authorise in these circumstances.

2.5.4 Authorising Officers should not ordinarily be responsible for authorising operations in which they are directly involved, although it is recognised that this may sometimes be unavoidable, especially in the case of small organisations.

2.5.5 Authorising Officers must complete the relevant part of the application form by hand, and forward the original to the Coordinating Officer within 1 week.

2.5.6 Authorising Officers must regularly review any applications they have authorised, and are responsible for cancellation of the same.

2.6 Covert Human Intelligence Source (CHIS)

2.6.1 A person is a CHIS if:

(a) they establish or maintain a personal or other relationship with a person for the covert purpose of facilitating the doing of anything falling within paragraph (b) or (c);

(b) they covertly use such a relationship to obtain information or to provide access to any information to another person;

(c) they covertly disclose information obtained by the use of such a relationship, or as a consequence of the existence of such a relationship.

2.7 **CHIS Controller**

2.7.1 The Controller is responsible for the management and supervision of the Handler, and general oversight of the use of the CHIS.

2.8 **CHIS Handler**

2.8.1 Handlers will usually be of a rank or position below that of Authorising Officer, and 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;
- monitoring the CHIS's security and welfare.

2.8.2 The CHIS Handler is responsible for bringing to the attention of the CHIS Controller any concerns about the personal circumstances of the CHIS, insofar as they might affect:

- the validity of the risk assessment;
- the conduct of the CHIS; and
- the safety and welfare of the CHIS.

3. SURVEILLANCE

3.1 **Surveillance** includes;

- monitoring, observing, or listening to persons, their movements, their conversations or their other activities or communications;
- recording anything monitored, observed, or listened to in the course of surveillance; and
- surveillance by or with the assistance of a surveillance device (meaning any apparatus designed or adapted for use in surveillance).

Surveillance can be either **overt** or **covert**.

3.2 **Overt Surveillance**

3.2.1 Most of the surveillance undertaken 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).

3.2.2 Similarly, surveillance will be overt if the person or persons subject to the surveillance are aware that it will happen, e.g., where a noisemaker is warned in writing that noise will be recorded if it continues, or where an entertainment licence is issued subject to conditions, and the licensee is told that Officers may visit without notice or without identifying themselves to the owner/proprietor to check that the conditions are being met.

3.3 Covert surveillance

3.3.1 Surveillance is covert where it is 'carried out in a manner calculated to ensure that the person or persons subject to the surveillance are unaware that it is or may be taking place'.

3.4 Directed Surveillance

3.4.1 Directed surveillance is surveillance which:

- is **covert**;
- is **not intrusive surveillance** (the Council must not carry out intrusive surveillance or interfere with private property (see below));
- is not carried out as an immediate response to events which would otherwise make seeking authorisation unreasonable, e.g. spotting something suspicious and continuing to observe it; and
- is undertaken for the purpose of a **specific investigation** or operation in a manner **likely to obtain private information** about an individual (whether or not that person is specifically targeted for purposes of an investigation).

3.4.2 *Private information* in relation to a person includes any information relating to his private and family life, his home and his correspondence. 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 they come into contact or associate with.

3.4.3 The way a person runs his/her business may also reveal information about his or her private life and the private lives of others.

3.4.4 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.

3.5 **Intrusive Surveillance**

3.5.1 Intrusive surveillance is surveillance which:

- is covert;
- is carried out in relation to anything taking place on any residential premises or in any private vehicle; and
- involves the presence of an individual on the premises or in the vehicle or is carried out by means of a surveillance device.

3.5.2 **Intrusive surveillance cannot be carried out or approved by the Council. Only the police and other law enforcement agencies are permitted to use such powers. Likewise, the Council has no statutory powers to interfere with private property.**

3.6 **Necessity**

3.6.1 RIPA requires that the person granting an Authorisation believe that it is necessary in the circumstances of the particular case. Therefore, applicants and Authorising Officers should consider why directed surveillance is **NECESSARY**. In addressing the issues of necessity in any particular case, information should include:

- Why directed surveillance is needed to obtain information that is sought from the operation?
- Why is it necessary to interfere with an individuals' privacy using covert surveillance?
- Why covert surveillance is the best option to obtain the information having considered other alternatives?
- What other methods of obtaining the information have been considered and why have they been discounted?

3.6.2 The Council cannot authorise directed surveillance unless the following conditions are met:

- The surveillance is for the purpose of preventing or detecting conduct which constitutes one or more criminal offences; and
- The criminal offence (or one of the criminal offences) is or would be punishable, whether on summary conviction or on indictment, by a maximum term of at least 6 months of imprisonment.

OR

- The criminal offence is an offence under:

- section 146 of the Licensing Act 2003 (sale of alcohol to children);
- section 147 of the Licensing Act 2003 (allowing the sale of alcohol to children);
- section 147A of the Licensing Act 2003 (persistently selling alcohol to children);
- section 7 of the Children and Young Persons Act 1933 (sale of tobacco, etc, to persons under eighteen).

3.7 **Proportionality**

3.7.1 If the directed surveillance is deemed to be necessary, the Authorising Officer must also believe that it is also proportionate to what is sought to be achieved. This involves balancing the seriousness of the intrusion into the privacy of the subject of the operation (or any other person who may be affected) against the need for the activity in investigative and operational terms.

3.7.2 The authorisation must not be 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.

3.7.3 No activity should be considered proportionate if the information sought could reasonably be obtained by other less intrusive means.

3.7.4 The following elements of proportionality should 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.

3.8 **Confidential Information**

3.8.1 Special safeguards apply with regard to confidential information. Confidential information consists of;

- *Communications subject to legal privilege*;
  A substantial proportion of the communications between a lawyer

and his client(s) may be subject to legal privilege.

- *Communications between a Member of Parliament and another person on constituency matters*;

  Confidential constituent information is information relating to communications between a Member of Parliament and a constituent in respect of constituency matters. Such information is held in confidence if it is held subject to an express or implied undertaking to hold it in confidence or it is subject to a restriction on disclosure or an obligation of confidentiality contained in existing legislation.

- *Confidential personal information*;

  Confidential personal information is information held in confidence relating to the physical or mental health or spiritual counselling concerning an individual (whether living or dead) who can be identified from it. Such information, which can include both oral and written communications, is held in confidence if it is held subject to an express or implied undertaking to hold it in confidence or it is subject to a restriction on disclosure or an obligation of confidentiality contained in existing legislation. Examples might include consultations between a health professional and a patient, or information from a patient's medical records.

- *Confidential journalistic material*.

  Confidential journalistic material includes material acquired or created for the purposes of journalism and held subject to an undertaking to hold it in confidence, as well as communications resulting in information being acquired for the purposes of journalism and held subject to such an undertaking.

3.8.2 Where it is anticipated that confidential information is likely to be collected as part of the surveillance, this can only be authorised by the Chief Executive or Monitoring Officer.

3.8.3 Where there is any doubt as to the handling and dissemination of confidential information, advice should be sought from the Senior Responsible Officer before any further dissemination of the material takes place.

3.9 **Collateral Intrusion**

3.9.1 Before authorising applications for directed surveillance, the Authorising Officer should also take into account the risk of obtaining private information about persons who are not subjects of the surveillance or operation (collateral intrusion).

3.9.2 Measures should be taken, wherever practicable, to avoid or minimise unnecessary intrusion into the privacy of those who are not the intended

subjects of the surveillance activity.

3.9.3 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 reauthorised or a new Authorisation is required.

3.10 Retention and Destruction of Material Obtained From Surveillance

3.10.1 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.

3.10.2 There is nothing in RIPA which 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.

4. COVERT HUMAN INTELLIGENCE SOURCES (CHIS)

4.1 Whilst it is theoretically possible that the Council may wish to establish a Covert Human Intelligence Source (CHIS) to act undercover, the instances when this will occur will be very rare indeed if ever. No CHIS should be considered without direct consultation with the Senior Responsible Officer.

4.2 Every CHIS must have an appointed Handler and Controller (see below).

4.3 Only the Chief Executive or Monitoring Officer can authorise a juvenile or vulnerable CHIS.

4.4 A risk assessment covering the health and safety of the CHIS must also be carried out.

4.5 What is a CHIS?

4.5.1 A person is a CHIS if:

(a) they establish or maintain a personal or other relationship with a person for the covert purpose of facilitating the doing of anything falling within paragraph (b) or (c);

(b) they covertly use such a relationship to obtain information or to provide access to any information to another person;

(c) they covertly disclose information obtained by the use of such a relationship, or as a consequence of the existence of such a relationship.

4.6 **What must be Authorised?**

4.6.1 The **conduct** or **use** of a CHIS requires prior authorisation.

4.6.2 **Use** of a CHIS involves any action on behalf of the Council to induce, ask or assist a person to engage in the conduct of a CHIS, or to obtain information by means of the conduct of a CHIS.

4.6.3 **Conduct** of a CHIS is any conduct of a CHIS falling within paragraph 4.5.1 above or is incidental to anything falling within the same.

4.6.4 Most CHIS Authorisations will be for both use and conduct. This is because public authorities usually take action in connection 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.

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

4.7 For the purpose of paragraph (d) of section 29(5) of RIPA, detailed records must be kept relating to each source. These are listed in Regulation 3 of the Regulation of Investigatory Powers (Source Records) Regulations 2000.

4.8 **Management of a CHIS**

4.8.1 Public authorities should ensure that arrangements are in place for the proper oversight and management of CHIS, including appointing individual officers as Controllers and Handlers for each CHIS.

4.8.2 Oversight and management arrangements for undercover operatives, while following the principles of the Act, will differ, in order to reflect the specific role of such individuals as members of public authorities.

4.8.3 **Tasking** is the assignment of the CHIS by the Handler or Controller, asking them to obtain, provide access to or disclose information.

4.8.4 Authorisations should not be drawn so narrowly that a separate Authorisation is required each time the CHIS is tasked. Rather, an Authorisation might cover, in broad terms, the nature of the CHIS's task.

4.8.5 Where it is intended to task a CHIS in a significantly greater or different way than previously identified in the Authorisation, the Handler or the Controller must refer the tasking to an Authorised Officer, who should consider whether the existing Authorisation is sufficient or needs

replacing.

4.8.6 The **Handler** will usually be of a rank or position below that of Authorising Officer, and 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;
- monitoring the CHIS's security and welfare.

4.8.7 The **Controller** will be responsible for the management and supervision of the Handler, and general oversight of the use of the CHIS.

4.9 Security and Welfare

4.9.1 When deploying a CHIS the Council should take into account the safety and welfare of the CHIS when carrying out actions in relation to an Authorisation or Tasking, and the foreseeable consequences to others of that Tasking.

4.9.2 Before Authorising the use of conduct of a CHIS, the Authorising Officer must ensure that a risk assessment is carried out to determine the risk to the CHIS of any Tasking and the likely consequences should the role of CHIS become known.

4.9.3 The ongoing security and welfare of the CHIS, after the cancellation of the Authorisation, should also be considered at the outset. Also, consideration should be given to the management of any requirement to disclose information tensing to reveal the existence or identity of a CHIS to, or in, court.

4.9.4 The CHIS Handler is responsible for bringing to the attention of the CHIS Controller any concerns about the personal circumstances of the CHIS, insofar as they might affect:

- the validity of the risk assessment;
- the conduct of the CHIS; and
- the safety and welfare of the CHIS.

4.9.5 Where appropriate, concerns about such matters must be considered by the Authorising Officer, and a decision taken on whether or not to allow the Authorisation to continue.

4.10 Record Keeping

4.10.1 A centrally retrievable record is held by the Coordinating Officer. These records need only contain the name, code name, or URN reference of the CHIS, and the date the Authorisation was granted, renewed or cancelled. These records must be updated whenever an Authorisation is granted, renewed or cancelled, and will be made available to the Investigatory Powers Commissioner or Inspector from the Investigatory Powers Commissioner's Office upon request. These records should be retained for a period of at least 3 years from the time the Authorisation ends.

4.10.2 While retaining records, the Council must take into consideration the duty of care to the CHIS, the likelihood of future criminal or civil proceedings relating to information supplied by the CHIS or activities undertaken, and any rules relating to data retention, review and deletion under the Data Protection Act etc.

4.10.3 Detailed records must also be kept of the Authorisation and use made of the CHIS. An Authorising Officer must not grant an Authorisation unless they believe that there are arrangements in place for ensuring that there is at all times a person with the responsibility for maintaining a record of the use made of the CHIS. The Regulation of Investigatory Powers (Source Records) Regulations 2000 detail the particulars that must be included.

4.11 **Juvenile Sources**

4.11.1 Special safeguards apply to the use or conduct of juvenile sources (i.e. those under 18 years old). On no occasion can a child under 16 years of age be authorised to give information against his or her parents. Only the Chief Executive or the Monitoring Officer are permitted to authorise the use of Juvenile CHIS.

4.12 The duration of such an Authorisation is one month from the time of grant or renewal (instead of 12 months). The age test is applied at the time of the grant or renewal of the Authorisation.

4.13 Vulnerable Individuals

4.13.1 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.

4.13.2 A Vulnerable Individual will only be authorised to act as a CHIS in the most exceptional circumstances. Only the Chief Executive or the Monitoring Officer are permitted to authorise the use of Vulnerable Individuals as a CHIS, as there are other onerous requirements for such matters, and the potential increased likelihood of harm to the vulnerable individual.

4.14 **Human Source Activity Falling Outside of CHIS**

4.14.1 Not all human source activity will fall within the definition of a CHIS. For example, a source may be a public volunteer who discloses information out of professional or statutory duty, or has been tasked to obtain information other than by way of relationship.

4.14.2 **Test Purchases** – Carrying out test purchases will not 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. For example, Authorisation would not normally be required for test purchases carried out in the ordinary course of business (e.g. walking into a shop and purchasing a product over the counter).

4.14.3 By contrast, developing a relationship with a person in the shop to obtain information about the seller's suppliers of an illegal product (e.g. illegally imported products) will require Authorisation as 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 CHIS and also directed surveillance.

4.14.4 **Anti-Social Behaviour** – 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.

4.14.5 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 in writing that this will occur if the level of noise continues. Placing a stationary or mobile video camera outside a building to record anti-social behaviour on residential estates will require prior Authorisation.

4.14.6 **Public Volunteers** – In many cases involving human sources, a relationship will not have been established or maintained for a covert purpose. Many sources merely volunteer or provide information that is within their personal knowledge, without being induced, asked, or tasked by a public authority. This means the source is not a CHIS for the purposes of RIPA and no Authorisation is required. For example, a member of the public may contact the Council and volunteer information regarding something they have witnessed in their neighbourhood.

4.14.7 **Professional or Statutory Duty** – Certain individuals will be required to provide information to public authorities or designated bodies out of professional or statutory duty. For example, employees within organisations regulated by money laundering legislation will be required to report suspicious transactions. Similarly, financial officials, accountants or company administrators may have a duty to provide information that they have obtained by virtue of their position to the Serious Fraud Office.

4.14.8 Furthermore, this reporting is undertaken 'in accordance with the law' and any action likely to interfere with an individual's privacy will not engage a person's human rights under Article 8.

4.14.9 This statutory or professional duty would not extend to a situation where a person is asked to provide information which they acquire as a result of an existing professional or business relationship with the subject but that person is under no obligation to pass it on. For example, a travel agent who is asked by the police to find out when a regular client next intends to fly to a particular destination is not under an obligation to pass this information on. In these circumstances a CHIS Authorisation may be appropriate.

4.15 Further Information

4.15.1 Further guidance on CHIS can be found in the Home Office Covert Human Intelligence Sources Code of Practice available at:

https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/97958/ code-practice-human-intel.pdf

5. COMMUNICATIONS DATA

5.1 Interception of Postal Items, Telephone Calls and Emails

5.1.1 Chapter I of Part I of RIPA deals with the interception of postal items, telephone calls and emails. Normally this requires a warrant issued by the Secretary of State. Exceptions exist where both sender and recipient consent, or where one of the parties consents and an authorisation under Part II of RIPA has been granted. Unlawful interception can be a criminal offence.

5.1.2 The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulation 2000 specifically authorise certain interceptions of telecommunications which would otherwise be prohibited by section 1 of RIPA. Regulation 3(1)(a) allows a business (which does include any public authority) to monitor its own internal communications system, including telephone calls, email messages and internet usage, for the following purposes (that are relevant to a local authority):

- To establish the existence of facts;
- To ascertain or demonstrate standards to be achieved (quality control and training);
- To prevent or detect crime;
- To investigate or detect unauthorised use of telecommunication systems; or
- To secure effective system operation.

5.1.3 These are far more wide ranging than the grounds normally available for directed surveillance under Part II of RIPA. It is therefore much easier to use the authority provided by the above stated Regulations, rather than the limited ones available under Part II of RIPA. The Regulations require that the Council make all reasonable efforts to inform potential users that interceptions may be made.

5.1.4 The Council has an Email Policy and Email usage guidelines. These describe the arrangements that the Council has in place for monitoring email communication. Informing members of staff of these policies and potential monitoring arrangements should be addressed within an employee's induction. Consent of the employee is not required for this monitoring however where employees are given facilities to make private telephone calls they should be given the opportunity to make calls without being monitored.

5.1.5 Where the Council monitor or record any telephone conversations the public need to be warned of this. This can be included as a footnote to entries in the telephone directory and on leaflets and advertisements. It can also be addressed through a recorded message or referred to specifically whenever the switchboard answers an incoming call. The purpose is ordinarily explained to be quality control and training. External emails are not normally intercepted during transmission, but are monitored only after they have arrived. Internal emails would be covered by the warning to members of staff. Internet access only involved the individual member of staff.

5.1.6 Further information about the interception of communications under RIPA can be found in the Home Office Interception of Communications Code of Practice at:

https://www.gov.uk/government/publications/interception-of-communications-code-of-practice-2016

5.2 **Acquisition and Disclosure of Communications Data**

5.2.1 Chapter II of Part I of RIPA covers the acquisition and disclosure of data held by any postal service or mobile telephone service about their customers. This is not directly relevant to local authorities as the data concerned is not relevant to the Councils' functions and powers.

5.2.2 Further information about the acquisition and disclosure of communications data under RIPA can be found in the Home Office Acquisition and Disclosure of Communications Data Code of Practice at:

https://www.gov.uk/government/publications/code-of-practice-for-the-acquisition-and-disclosure-of-communications-data

6. AUTHORISATION PROCEDURES

6.1 Directed Surveillance and the use of CHIS can only be lawfully carried out

if properly authorised, and in strict accordance with the terms of the Authorisation. **Appendix C (Directed Surveillance) and Appendix E (CHIS)** provide flow charts of processes from application/consideration to recording of information and the storage/retention of data obtained.

6.2 **Authorising Officers**

6.2.1 Forms can only be signed by appointed Authorising Officers. Authorised posts are listed in **Appendix A**. This Appendix will be kept up to date and added to as needs require. If a Chief Officer wishes to add, delete or substitute a post, s/he must refer such request to the Director (LD) for consideration, as necessary. The Director (LD) has been duly authorised to add, delete or substitute posts listed in **Appendix A**.

6.2.2 Authorisations under RIPA are separate from delegated authority to act under the Council's Scheme of Delegation and internal departmental Schemes of Delegation. All RIPA Authorisations, save for Authorisations to collect communications data under s22 (3) RIPA, are for specific investigations only, and must be reviewed, renewed or cancelled once the specific surveillance is complete or about to expire. **The authorisations do not lapse with time!**

6.3 **Training Records**

6.3.1 Appropriate training will be given (or approved) before Authorising Officers are certified to sign any RIPA Forms. A record of training will be retained and a Central Register of all those individuals who have undergone training (or a one-to-one meeting) on such matters will be kept.

6.3.2 If the Senior Responsible Officer feels that an Authorising Officer has not complied fully with the requirements of this Document, or the training provided to him/her, they are duly authorised to retract that Officer's authorisation until s/he has undertaken further approved training or a one-to-one meeting.

6.4 **Application Forms**

6.4.1 Application Forms **must be hand written** and not typed.

6.4.2 Only the RIPA forms below or contained on the Home Office website are permitted to be used. Any other forms used will be rejected.

6.4.3 **A Forms (Directed Surveillance) – Appendix C**

FORM	DESCRIPTION	PAGE
A1	Application for Authority for Directed Surveillance	43
A2	Review of Directed Surveillance Authority	48
A3	Renewal of Directed Surveillance Authority	52
A4	Cancellation of Directed Surveillance Authority	56

6.4.4 **B Forms (CHIS) – Appendix F**

FORM	DESCRIPTION	PAGE
B1	Application for Authority for Conduct and Use of CHIS	64
B2	Review of Conduct and Use of CHIS	70
B3	Renewal of Conduct and Use of CHIS	74
B4	Cancellation of Conduct and Use of CHIS	78

6.5 **Grounds for Authorisation**

6.5.1 The Council cannot authorise Directed Surveillance unless the following conditions are met:

- The surveillance is for the purpose of preventing or detecting conduct which constitutes one or more criminal offences; and
- The criminal offence (or one of the criminal offences) is or would be punishable, whether on summary conviction or on indictment, by a maximum term of at least 6 months of imprisonment.

OR

- The criminal offence is an offence under:
    - section 146 of the Licensing Act 2003 (sale of alcohol to children);
    - section 147 of the Licensing Act 2003 (allowing the sale of alcohol to children);
    - section 147A of the Licensing Act 2003 (persistently selling alcohol to children);
    - section 7 of the Children and Young Persons Act 1933 (sale of tobacco, etc, to persons under eighteen).

6.5.2 The Council cannot authorise directed surveillance on any other grounds

(no other grounds are available to local authorities). There is however no such restriction on the use of CHIS.

6.6 **Assessing the Application Form**

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

(a) Be mindful of this Document, the training provided and any other guidance issued from time to time on such matters;

(b) Satisfy themselves that:

(i) the RIPA Authorisation is in accordance with the law;

(ii) the offence falls within the categories listed at 5.5.1;

(iii) the Authorisation is necessary in the circumstances of the particular case; and

(iv) the Authorisation is proportionate to what it seeks to achieve.

(c) In assessing whether or not the proposed surveillance is proportionate, consider whether there are any other non-intrusive means of obtaining information, 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.**

(d) Take into account the risk of intrusion into the privacy of persons other than the specified subject of the surveillance (collateral intrusion). Measures must be taken wherever practicable to avoid or minimise (so far as is possible) collateral intrusion and the matter may be an aspect of determining proportionality.

(e) Set a date for review of the Authorisation and review on that date using the appropriate form.

(f) Obtain a unique reference number (URN) for each form in the format: Year/Dept/Number of Application. The Coordinating Officer will supply the URN.

(g) Ensure that any RIPA Departmental Register is duly completed, and that the **original** RIPA Forms (and any review / renewal / cancellation of the same) are forwarded to the Coordinating Officer, **within 1 week of the relevant authorisation, review, renewal, cancellation or rejection**.

(h) If unsure on any matter, obtain advice from the Senior Responsible Officer or the Coordinating Officer before signing any forms.

6.6.2 When Authorising the use or conduct of a **CHIS**, the 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 risk assessment;

(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 unsure on any matter, obtain advice from the Senior Responsible Officer or the Coordinating Officer before signing any forms.

6.7 **Approval by a Justice of the Peace**

6.7.1 The Protection of Freedoms Act 2012 amended RIPA so that **all local authority authorisations are subject to judicial approval**. This means that the Council must obtain an order of a Justice of the Peace (JP) at the Magistrates' Court approving the grant or renewal of an authorisation before it can take effect.

6.7.2 Although it is theoretically possible for local authorities to request judicial approval for the use of more than one technique (i.e. Directed Surveillance, CHIS and Communications Data) at the same time, in practice, as different considerations need to be applied to these different techniques, this would be difficult to perform with the degree of clarity required. Separate Authorisations or notices to use different RIPA techniques should therefore be submitted.

6.7.3 It should be noted that only the **initial application** and any **renewal of the application** require magistrates' approval. Review and cancellation of Authorisations do not require such judicial approval and remain an internal process.

6.8 **The Role of the Justice of the Peace**

6.8.1 The role of the JP is set out in RIPA. Section 23A of RIPA covers this role in relation to communications data, and section 32A covers this role in relation to applications for directed surveillance and CHIS.

6.8.2 These provisions state that the Authorisation (or in the case of communications data the notice) shall not take effect until the JP has made an order approving grant of the Authorisation or notice.

6.8.3 The matters on which a JP must be satisfied before making an order of approval are:

- There were reasonable grounds for believing that the Authorisation is necessary and proportionate and that these grounds remain at the time of consideration by the JP;

- In relation to a CHIS, that there were also reasonable grounds to believe that arrangements exist for the safety and welfare of the source that satisfy section 29(5) RIPA and that these grounds remain at the time of consideration by the JP;

- In relation to a juvenile CHIS, that there were reasonable grounds to believe that the requirements imposed by Regulation of Investigatory Powers (Juveniles) Order 2003 were satisfied and that these grounds remain at the time of consideration by the JP.

- The application has been properly authorised by a designated person;

- The grant of Authorisation (or in the case of communications data the notice) was not in breach of any restrictions imposed pursuant to sections 25(3), 29(7)(a), or 30(3) of RIPA.

6.9 **Urgent Authorisations**

6.9.1 Due to the fact that an authorisation under RIPA cannot take effect until approved by a JP, **urgent oral authorisations can no longer be granted**. There is no exception to this rule.

6.10 **Duration**

6.10.1 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 a maximum of 3 months (from Authorisation) for Directed Surveillance, and 12 months (from Authorisation) for a CHIS (or one month if 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).

6.10.2 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.

6.10.3 The renewal will begin on the day when the Authorisation would have expired

.

7. WORKING WITH OTHER AGENCIES

7.1 When another 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.

7.2 Where another Agency (e.g. Police, Customs & Excise, Inland Revenue 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, they must obtain a copy of that agency's RIPA form for the record (a copy of which must be passed to the Coordinating Officer for the Central Register) or relevant extracts from the same which are sufficient for the purposes of protecting the Council and the use of its resources.

(b) wish to use the Council's premises for their own RIPA action, and is expressly seeking assistance from the Council, the Officer should normally co-operate with the same, unless there are security or other good operational or managerial reasons as to why the Council's premises should not be used for the agency's activities. Suitable insurance or other appropriate indemnities may be sought, if necessary, from the other Agency for the Council's co-operation in the 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.

7.3 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.

7.4 **If in doubt, please consult with the Senior Responsible Officer at the earliest opportunity, and in any case prior to making resources available.**

COVERT SURVEILLANCE OF SOCIAL NETWORKING SITES

7.5 The growing popularity of social media (such as Facebook and Twitter) has resulted in more and more people publishing information about themselves and their activities on the internet.

7.6 This source of information can be very useful and is relatively easy to access, however caution must be exercised when doing so for the

purpose of surveillance activity. In particular, care must be taken to understand how the social networking site being used works. Authorising Officers must not be tempted to assume that one service provider is the same as another or that the services provided by a single provider are the same.

7.7 Where the individual has applied privacy controls to the information, so that it is not publicly available, it would be unwise to consider the information as "open source". The author has a reasonable expectation of privacy if access controls are applied.

7.8 Where privacy controls are available but have not been applied, the information may be considered "open source" and an authorisation would not normally be required. That said, in the view of the Surveillance Commissioner repeat viewing of "open source" sites may constitute directed surveillance on a case by case basis and this should be borne in mind.

7.9 If it is necessary and proportionate for the Council to covertly breach access controls, the minimum requirement is an Authorisation for directed surveillance.

7.10 An Authorisation for the use and conduct of a CHIS is necessary if a relationship is established or maintained (i.e. the activity is more than mere reading of the site's content).

7.11 In undertaking covert surveillance of this type, the identity of a person known, or likely to be known, to the subject of interest or users of the site should not be adopted without authorisation, without the consent of the person whose identity is used, and without considering the protection of that person. Consent must be explicit and in writing.

7.12 Should an Officer be considering surveillance of this type, they are urged to consult with the Senior Responsible Officer or the Coordinating Officer before taking any further steps.

8. RECORDS MANAGEMENT

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

8.2 Records Maintained by the Department

9.2.1 The Council will retain records for a period of at least three years from the ending of the Authorisation. The IPCO can audit/review the Council's policies and procedures, and individual Authorisations, Reviews, Renewals, Cancellations and rejections. Records must include the following information:

- A copy of the Forms together with any supplementary documentation and notification of the approval given by the Authorising Officer;

- A record of the period over which the surveillance has taken place;

- The frequency of reviews prescribed by the Authorising Officer;

- A record of the result of each review of the Authorisation;

- A copy of any renewal of an Authorisation, together with the supporting documentation submitted when the renewal was requested;

- The date and time when any instruction was given by the Authorising Officer;

- The Unique Reference Number for the Authorisation (URN).

9.3 **Central Register Maintained by the Director (LD)**

9.3.1 For Directed Surveillance, the Central Register is administered by the Coordinating Officer. For CHIS applications, Authorising Officers must forward originals of each Form B to the Coordinating Officer for the Central Register, within 1 week of the authorisation, Review, Renewal, Cancellation or rejection. The Coordinating Officer will monitor the same and give appropriate guidance, from time to time, or amend this Document as necessary.

9. CONCLUDING REMARKS

9.1 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 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.

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

9.3 **Authorising Officers will be suitably trained and they 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. All forms must be hand written.**

9.4 **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. Reasons for any refusal of an application must also be kept on the form and the form retained for future audits.

9.5 For further advice and assistance on RIPA, please contact the Senior Responsible Officer or the Coordinating Officer. Details are provided on the front of this Document.

APPENDIX A

SENIOR RESPONSIBLE OFFICER

Director of (LD) (Monitoring Officer)

AUTHORISING OFFICERS

Chief Executive

Director (LD) (Monitoring Officer)

Director (NE)

Director (RB)

COORDINATING OFFICER

Deputy Monitoring Officer

IMPORTANT NOTES:

A. Even if a post is identified in the above list the persons currently employed in such posts are not authorised to sign RIPA Forms (including a review, renewal or cancellation) unless they have been certified by the Director (LD) to do so.

B. Only the Chief Executive and the Monitoring Officer are authorised to sign Forms relating to Juvenile Sources and Vulnerable Individuals or where there is any possibility of confidential information being obtained.

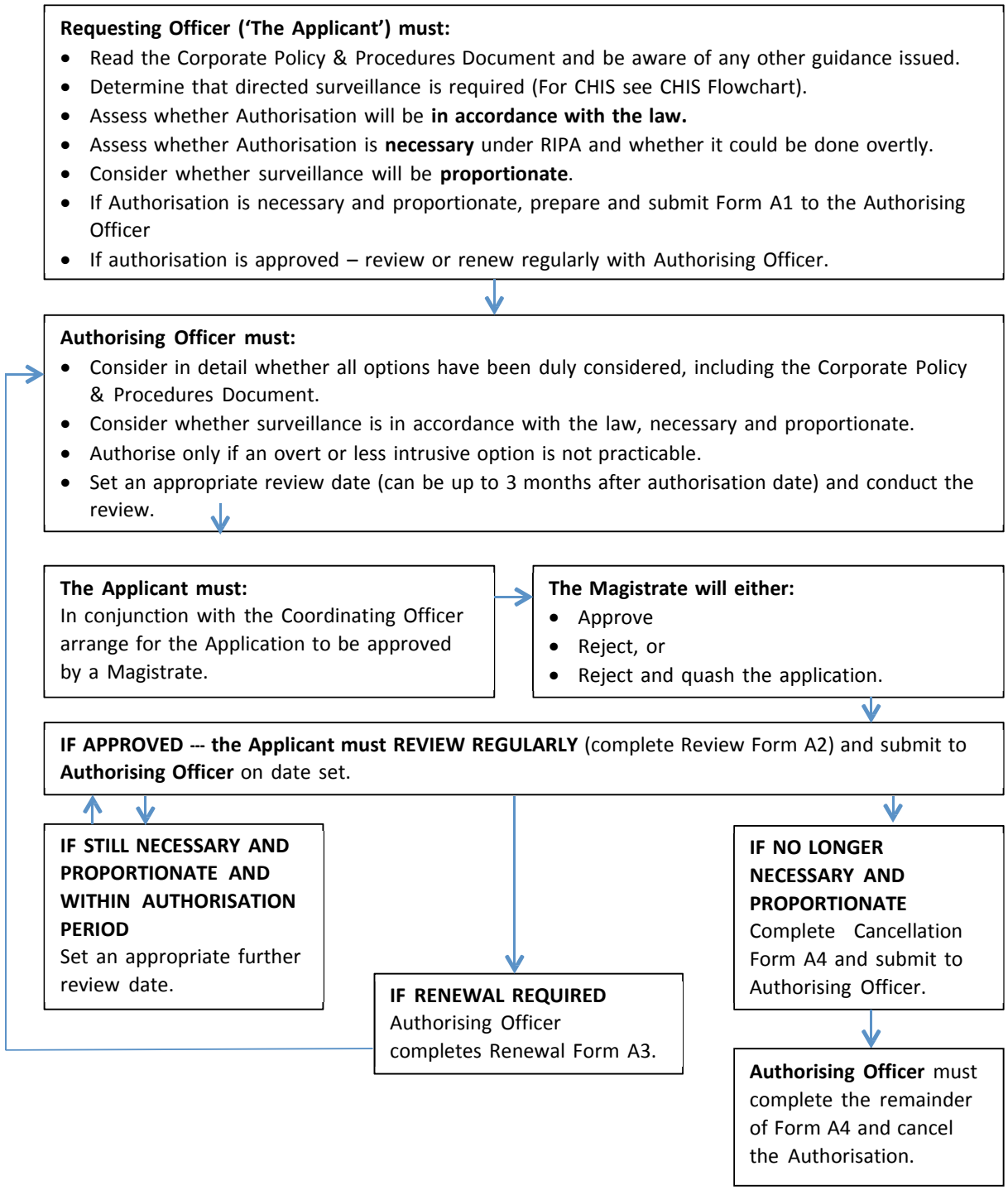
C. The Director (LD) should only act as an Authorising Officer in exceptional circumstances.

D. If a Chief Officer wishes to add, delete or substitute a post, they must refer such request to the Director (LD) for consideration, as necessary.

E. If in doubt, ask the Senior Responsible Officer or the Coordinating Officer BEFORE any directed surveillance and/or CHIS is authorised, reviewed, renewed, cancelled or rejected.

F. APPENDIX B

DIRECTED SURVEILLANCE FLOW CHART



If in doubt, consult the Senior Responsible Officer or the Coordinating Officer BEFORE any directed surveillance and/or CHIS are Authorised, Reviewed, Renewed, Cancelled, or rejected.

APPENDIX C

RIPA 'A' FORMS – DIRECTED SURVEILLANCE

Form	Description
A1	Application for Authorisation to carry out directed surveillance
A2	Review of Form A1
A3	Application for Renewal of Form A1
A4	Cancellation of Form A1

ALL FORMS MUST BE COMPLETED BY HAND

FORM A1 – APPLICATION FOR AUTHORISATION TO CARRY OUT DIRECTED SURVEILLANCE

PART II REGULATION OF INVESTIGATORY POWERS ACT 2000

SCARBOROUGH BOROUGH COUNCIL

STRICTLY PRIVATE AND CONFIDENTIAL

TO BE COMPLETED BY HAND

Unique Reference Number (URN)	
Subject of Surveillance (including full address)	

SECTION 1 (TO BE COMPLETED BY APPLICANT)

Name of Applicant		**Unit/Service**	
Full Address			
Contact Details			
Investigation/Operation Name (if applicable)			
Investigating Officer (if person other than the Applicant)			

Details of Application

1. Give name and job title of Authorising Officer

2. Describe the purpose of the specific operation or investigation.
3. Describe in detail the surveillance operation to be authorised and expected duration, including any premises, vehicles or equipment (e.g. camera, binoculars, recorder) that may be used.
4. The identities, where known, of those to be subject of the directed surveillance.
• Name: • Address: • DOB: • Other information as appropriate:

5. Explain the information that it is desired to obtain as a result of the directed surveillance.
6. Explain why directed surveillance is NECESSARY in this particular case:
CRIME(S) BEING INVESTIGATED: **MAXIMUM PENAL PROVISIONS (MUST BE MAX OF AT LEAST 6 MONTHS IMPRISONMENT):** **NB: UNDER SECTION 28 OF RIPA, THE ONLY GROUND AVAILABLE TO THE COUNCIL IS "FOR THE PURPOSE OF PREVENTING OR DETECTING CRIME". THIS APPLICATION MUST BE REJECTED IF THIS GROUND IS NOT RELEVANT TO THE PROPOSED SURVEILLANCE**
7. Supply details of any potential COLLATERAL INTRUSION and why the intrusion is unavoidable: (Also describe precautions to MINIMISE collateral intrusion)

8. Explain why the directed surveillance is PROPORTIONATE to what it seeks to achieve. How intrusive might it be on the subject of surveillance or on others? And why is this intrusion outweighed by the need for surveillance in operational terms or can the evidence be obtained by any other means?
9. Confidential information (e.g. confidential legal privilege, personal information and journalistic material) INDICATE THE LIKELIHOOD OF ACQUIRING ANY CONFIDENTIAL INFORMATION

10. Applicant's Details	
Name:	**Tel No:**
Job Title:	**Date:**
Signature:	

11. Anticipated Start Date and Time	
Date:	**Time:**

SECTION 2 (TO BE COMPLETED BY AUTHORISING OFFICER)

12. Authorising Officer's Statement **MUST spell out the "5 Ws" – Who; What; Where; When; Why and HOW**
I hereby authorise as follows: *Who is authorised to conduct surveillance:* *What is authorised for the surveillance:* *Where is it to take place and for how long:* *Why is it being authorised:* *How will the surveillance be conducted:* This written authorisation will cease to have effect at the end of a period of 3 months unless renewed (see separate form for renewals).

The Applicant and the **Authorising** Officer will jointly review this authorisation on the date below to see whether the authorisation should continue, be renewed or cancelled.
13. Authorising Officer's statement explaining why in his / her view the directed surveillance is necessary and proportionate. This box must be completed and both aspects must be addressed.
Why is it necessary? Why is it proportionate?
14. Confidential Information Authorisation. Supply details demonstrating compliance with Home Office Codes of Practice relating to this issue.

Expiry of Authorisation (3 months from date / time of Authorisation unless stated here):	
Date of first review:	
Date of subsequent reviews of this Authorisation:	

Authorising Officer	
Job Title	
Signature	
Date/Time	

NB: The original copy of this form, once it has been authorised or rejected, must be sent to the Coordinating Officer within 1 week of the authorisation or rejection for placing in the Central Register.

FORM A2 – REVIEW OF A DIRECTED SURVEILLANCE AUTHORISATION

PART II REGULATION OF INVESTIGATORY POWERS ACT 2000

SCARBOROUGH BOROUGH COUNCIL

STRICTLY PRIVATE AND CONFIDENTIAL

TO BE COMPLETED BY HAND

Unique Reference Number (URN)	
Subject of Surveillance (including full address)	

SECTION 1 (TO BE COMPLETED BY APPLICANT)

Name of Applicant		**Unit/Service**	
Full Address			
Contact Details			
Investigation/Operation Name (if applicable)			
Investigating Officer (if person other than the Applicant)			
Date of Authorisation or Last Renewal			
Expiry Date of Authorisation or Last Renewal			

Details of Review

1. Review Number and Dates of any Previous Reviews	
Review Number	**Dates**

2.	**Summary of the investigation/operation to date, including what private information has been obtained and the value of the information so far obtained**
3.	**Detail the reasons why it is NECESSARY to continue with the directed surveillance**
4.	**Explain how the proposed activity is still PROPORTIONATE to what it seeks to achieve**
5.	**Detail any incidents of collateral intrusion and the likelihood of any further incidents of collateral intrusions occurring**

6. Give details of any confidential information acquired or accessed and the likelihood of acquiring confidential information

7. Applicant's Details	
Name:	**Tel No:**
Job Title:	**Date:**
Signature:	

SECTION 2 (TO BE COMPLETED BY AUTHORISING OFFICER)

8. Authorising Officer's Comments, including whether or not the directed surveillance should continue

9. Authorising Officer's Statement
I [hereby agree that the directed surveillance investigation/operation as detailed above [should/should not] continue [until its next review/renewal][it should be cancelled immediately].

Authorising Officer	
Job Title	
Signature	
Date/Time	

10. Date of Next Review	

NB: The original copy of this form, once it has been authorised or rejected, must be sent to the Coordinating Officer within 1 week of the authorisation or rejection for placing in the Central Register.

FORM A3 – APPLICATION FOR RENEWAL OF A DIRECTED SURVEILLANCE AUTHORISATION
(Please attach a copy of the original authorisation)

PART II REGULATION OF INVESTIGATORY POWERS ACT 2000

SCARBOROUGH BOROUGH COUNCIL

STRICTLY PRIVATE AND CONFIDENTIAL

TO BE COMPLETED BY HAND

Unique Reference Number (URN)	
Subject of Surveillance (including full address)	

SECTION 1 (TO BE COMPLETED BY APPLICANT)

Name of Applicant		**Unit/Service**	
Full Address			
Contact Details			
Investigation/Operation Name (if applicable)			
Investigating Officer (if person other than the Applicant)			
Date of Authorisation or Last Renewal			
Expiry Date of Authorisation or Last Renewal			
Renewal Number			

Details of Renewal

1. Renewal Number and Dates of any Previous Renewals	
Renewal Number	**Dates**

2. Detail any significant changes to the information provided in the original authorisation, as it applies at the time of the renewal

3. Detail the reasons why it is NECESSARY to continue with the directed surveillance

4. Explain how the proposed activity is still PROPORTIONATE to what it seeks to achieve

5. Indicate the content and value to the investigation or operation of the information so far obtained by the directed surveillance

6. Give details of the results of the regular reviews of the investigation or operation

7. Applicant's Details	
Name:	**Tel No:**
Job Title:	**Date:**
Signature:	

SECTION 2 (TO BE COMPLETED BY AUTHORISING OFFICER)

8. Authorising Officer's Comments This box must be completed to indicate why the renewal (if agreed) is necessary and proportionate
9. Authorising Officer's Statement
I hereby authorise the renewal of the directed surveillance operation as detailed above. The renewal of this authorisation will last for 3 months unless renewed in writing. This authorisation will be reviewed frequently to assess the need for the authorisation to continue.

Authorising Officer	
Job Title	
Signature	
Date/Time	

10. Date of First Review	
11. Date of Subsequent Reviews of this Authorisation	

NB: The original copy of this form, once it has been authorised or rejected, must be sent to the Coordinating Officer within 1 week of the authorisation or rejection for placing in the Central Register.

FORM A4 – APPLICATION FOR CANCELLATION OF A DIRECTED SURVEILLANCE AUTHORISATION

PART II REGULATION OF INVESTIGATORY POWERS ACT 2000

SCARBOROUGH BOROUGH COUNCIL

STRICTLY PRIVATE AND CONFIDENTIAL

TO BE COMPLETED BY HAND

Unique Reference Number (URN)	
Subject of Surveillance (including full address)	

SECTION 1 (TO BE COMPLETED BY APPLICANT)

Name of Applicant		**Unit/Service**	
Full Address			
Contact Details			
Investigation/Operation Name (if applicable)			
Investigating Officer (if person other than the Applicant)			
Date of Authorisation or Last Renewal			
Expiry Date of Authorisation or Last Renewal			

Details of Cancellation

1. Explain the reasons for the Cancellation of the Authorisation

2. Explain the value of surveillance in the operation:

3. Applicant's Details	
Name:	**Tel No:**
Job Title:	**Date:**
Signature:	

SECTION 2 (TO BE COMPLETED BY AUTHORISING OFFICER)

4. Authorising Officer's Statement
I hereby authorise the cancellation of the directed surveillance investigation/operation as detailed above.

Authorising Officer	
Job Title	
Signature	
Date/Time	

5. Time and Date of when the Authorising Officer instructed the surveillance to cease			
Date:		**Time:**	

6. Authorisation cancelled	Date:	Time:

NB: The original copy of this form, once it has been authorised or rejected, must be sent to the Coordinating Officer within 1 week of the authorisation or rejection for placing in the Central Register.

APPENDIX D
COVERT HUMAN INTELLIGENCE SOURCE (CHIS)

Additional Notes (an extract from the Home Office Code of Practice on CHIS)
Management of Covert Human Intelligence Sources

Tasking

6.1 Tasking is the assignment given to the CHIS by the persons defined at sections 29(5)(a) and (b) of the 2000 Act, asking him to obtain, provide access to or disclose information. Authorisation for the use or conduct of a CHIS will be appropriate prior to any tasking where such tasking involves the CHIS establishing or maintaining a personal or other relationship for a covert purpose.

6.2 Authorisations should not be drawn so narrowly that a separate authorisation is required each time the CHIS is tasked. Rather, an authorisation might cover, in broad terms, the nature of the source's task. If there is a step change in the nature of the task that significantly alters the entire deployment, then a new authorisation may need to be sought. If in doubt, advice should be sought from the Investigatory Powers Commissioner.

6.3 It is difficult to predict exactly what might occur each time a meeting with a CHIS takes place, or the CHIS meets the subject of an investigation. There may be occasions when unforeseen action or undertakings occur. When this happens, the occurrence must be recorded as soon as practicable after the event, and if the existing authorisation is insufficient, it should either be reviewed and updated (for minor amendments only) or it should be cancelled and a new authorisation should be obtained before any further such action is carried out.

6.4 Similarly, where it is intended to task a CHIS in a significantly greater or different way than previously identified, the persons defined at section 29(5)(a) or (b) of the 2000 Act must refer the proposed tasking to the authorising officer, who should consider whether the existing authorisation is sufficient or needs to be replaced. This should be done in advance of any tasking and the details of such referrals must be recorded. Efforts should be made to minimise the number of authorisations per CHIS to the minimum necessary in order to avoid generating excessive paperwork.

Handlers and controllers

6.5 Public authorities should ensure that arrangements are in place for the proper oversight and management of CHIS, including appointing individual officers acting as 'controller' and 'handler' for each CHIS (as defined in sections 29(4A) and (4B) and 29(5)(a) and (b) of the 2000 Act).

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

- dealing with the CHIS on behalf of the authority concerned;
- directing the day to day activities of the CHIS;
- recording the information supplied by the CHIS; and
- monitoring the CHIS's security and welfare.

6.7 The handler of a CHIS will usually be of a rank or position below that of the authorising officer.

6.8 The person referred to in section 29(5)(b) of the 2000 Act (the “controller”) will normally be responsible for the management and supervision of the “handler” and general oversight of the use of the CHIS.

6.9 Oversight and management arrangements for undercover operatives, while following the principles of the Act, will differ, in order to reflect the specific role of such individuals as members of public authorities. The role of the handler will be undertaken by a person referred to as a ‘cover officer’ and the role of controller will be undertaken by a ‘covert operations manager’.

Joint working

6.10 There are many cases where the activities of a CHIS may provide benefit to more than a single public authority. Such cases may include:

- The prevention or detection of criminal matters affecting a national or regional area, for example where the CHIS provides information relating to cross boundary or international drug trafficking;
- The prevention or detection of criminal matters affecting crime and disorder, requiring joint agency operational activity, for example where a CHIS provides information relating to environmental health issues and offences of criminal damage, in a joint police/local authority anti-social behaviour operation on a housing estate;
- Matters of national security, for example where the CHIS provides information relating to terrorist activity and associated criminal offences for the benefit of the police and the Security Service.

6.11 In cases where the authorisation is for the use or conduct of a CHIS whose activities benefit more than a single public authority, responsibilities for the management and oversight of that CHIS may be taken up by one authority or can be split between the authorities. The applicant, controller and handler of a CHIS need not be from the same public authority. In such situations, however, the public authorities involved must lay out in writing their agreed oversight arrangements.

6.12 Management responsibility for CHIS, and relevant roles, may also be divided between different police forces and the National Crime Agency where there is a collaboration agreement under the Police Act 1996 and the collaboration agreement provides for this to happen.

Security and welfare

6.13 Any public authority deploying a CHIS should take into account the safety and welfare of that CHIS when carrying out actions in relation to an authorisation or tasking, and the foreseeable consequences to others of that tasking. Before authorising the use or conduct of a CHIS, the authorising officer should ensure that a risk assessment is carried out to determine the risk to the CHIS of any tasking and the likely consequences should the role of the CHIS become known. This should consider the risks relating to the specific tasking and circumstances of each authorisation separately, and should be updated to reflect developments during the course of the deployment, as well as after the deployment if contact is maintained. The ongoing security and welfare of the CHIS, after the cancellation of the authorisation, should also be considered at the outset and reviewed throughout the period of authorised activity by that CHIS. Consideration should also be given to the management of any requirement to disclose information which could risk revealing the existence or identity of a CHIS. For example this could be by means of disclosure to a court

or tribunal, or any other circumstances where disclosure of information may be required, and strategies for minimising the risks to the CHIS or others should be put in place. Additional guidance about protecting the identity of the CHIS is provided at paragraphs 8.22 to 8.25 below.

6.14 The CHIS handler is responsible for bringing to the attention of the CHIS controller any concerns about the personal circumstances of the CHIS, insofar as they might affect:

• the validity of the risk assessment;

• the conduct of the CHIS; and

• the safety and welfare of the CHIS.

6.15 Where appropriate, concerns about such matters must be considered by the authorising officer, and a decision taken on whether or not to allow the authorisation to continue

SENIOR RESPONSIBLE OFFICERS AND OVERSIGHT BY COMMISSIONERS

The Senior Responsible Officer

9.1 Within every relevant public authority a senior responsible officer must be appointed with responsibility for:

- the integrity of the process in place within the public authority for the management of CHIS;
- compliance with Part II of the Act and with this code;
- oversight of the reporting of errors to the Investigatory Powers Commissioner and the identification of both the cause(s) of errors and the implementation of processes to minimise repetition of errors;
- engagement with the Investigatory Powers Commissioner and inspectors who support the Commissioner when they conduct their inspections, ;
- where necessary, oversight of the implementation of post-inspection action plans recommended or approved by the Investigatory Powers Commissioner; and
- ensuring that all authorising officers are of an appropriate standard, addressing any recommendations and concerns in the inspection reports prepared by the Investigatory Powers Commissioner

Oversight by Commissioners

9.2 The Investigatory Powers Act provides for an Investigatory Powers Commissioner ("the Commissioner"), whose remit includes providing comprehensive oversight of the use of the powers to which this code applies, and adherence to the practices and processes described in it. The Commissioner will be, or will have been, a member of the senior judiciary and will be entirely independent of Her Majesty's Government or any of the public authorities authorised to use investigatory powers. The Commissioner will be supported by inspectors and others, such as technical experts, qualified to assist the Commissioner in his or her work. The Commissioner will also be advised by the 'Technology Advisory Panel'.

9.3 The Commissioner, and those that work under the authority of the Commissioner, will ensure compliance with the law by inspecting public authorities and investigating any issue which they believe warrants further independent scrutiny. The Investigatory Powers Commissioner may undertake these inspections, as far as they relate to the Investigatory Powers Commissioner's statutory functions, entirely on his or her own initiative, or the Commissioner may be asked to investigate a specific issue by the Prime Minister. Section 236 of the 2016 Act also provides for the Intelligence and Security Committee of Parliament to refer a matter to the Investigatory Powers Commissioner with a view to carrying out an investigation, inspection or audit.

9.4 The Commissioner will have unfettered access to all locations, documentation and information systems as necessary to carry out their full functions and duties. In undertaking such inspections, the Investigatory Powers Commissioner must not act in a way which is contrary to the public interest or prejudicial to national security, the prevention or detection of serious crime, or the economic well-being of the UK (section 229(6) of the 2016 Act). A Commissioner must in particular not jeopardise the success of an intelligence, security or law enforcement operation, compromise the safety or security of those involved, nor unduly impede the operational effectiveness of an intelligence service, a police force, a government department, or Her Majesty's Forces (see section 229(7) of the 2016 Act).

9.5 All relevant persons using investigatory powers must provide all necessary assistance to the Commissioner and anyone who is acting on behalf of the Commissioner. Here, a relevant person includes, amongst others, any person who holds, or has held, an office, rank or position within a public authority (see section 235(7) of the 2016 Act).

9.6 Anyone, including anyone working for a public authority, who has concerns about the way that investigatory powers are being used may report their concerns to the Commissioner. In particular, any person who exercises the powers described in this code must, in accordance with the procedure set out in chapter 7 of this code, report to the Commissioner any relevant error of which they are aware. This may be in addition to the person raising concerns through the internal mechanisms for raising concerns within the public authority.

9.7 Should the Commissioner uncover, or be made aware of, what they consider to be a serious error relating to a person who has been subject to an investigatory power then, if it is in the public interest to do so, the Commissioner is under a duty to inform the person affected. Further information on errors can be found in chapter 8 of this code. The public authority that has made the error will be able to make representations to the Commissioner before the Commissioner decides if it is in the public interest for the person to be informed. Section 231(6) of the 2016 Act states that the Commissioner must also inform the affected person of their right to apply to the Investigatory Powers Tribunal (see chapter 10 of this code for more information on how this can be done).

9.8 The Commissioner must report annually on the findings of their audits, inspections and investigations. This report will be laid before Parliament and will be made available to the public, subject to any necessary redactions made in the public interest. Only the Prime Minister will be able to make redactions to the Commissioner's report.

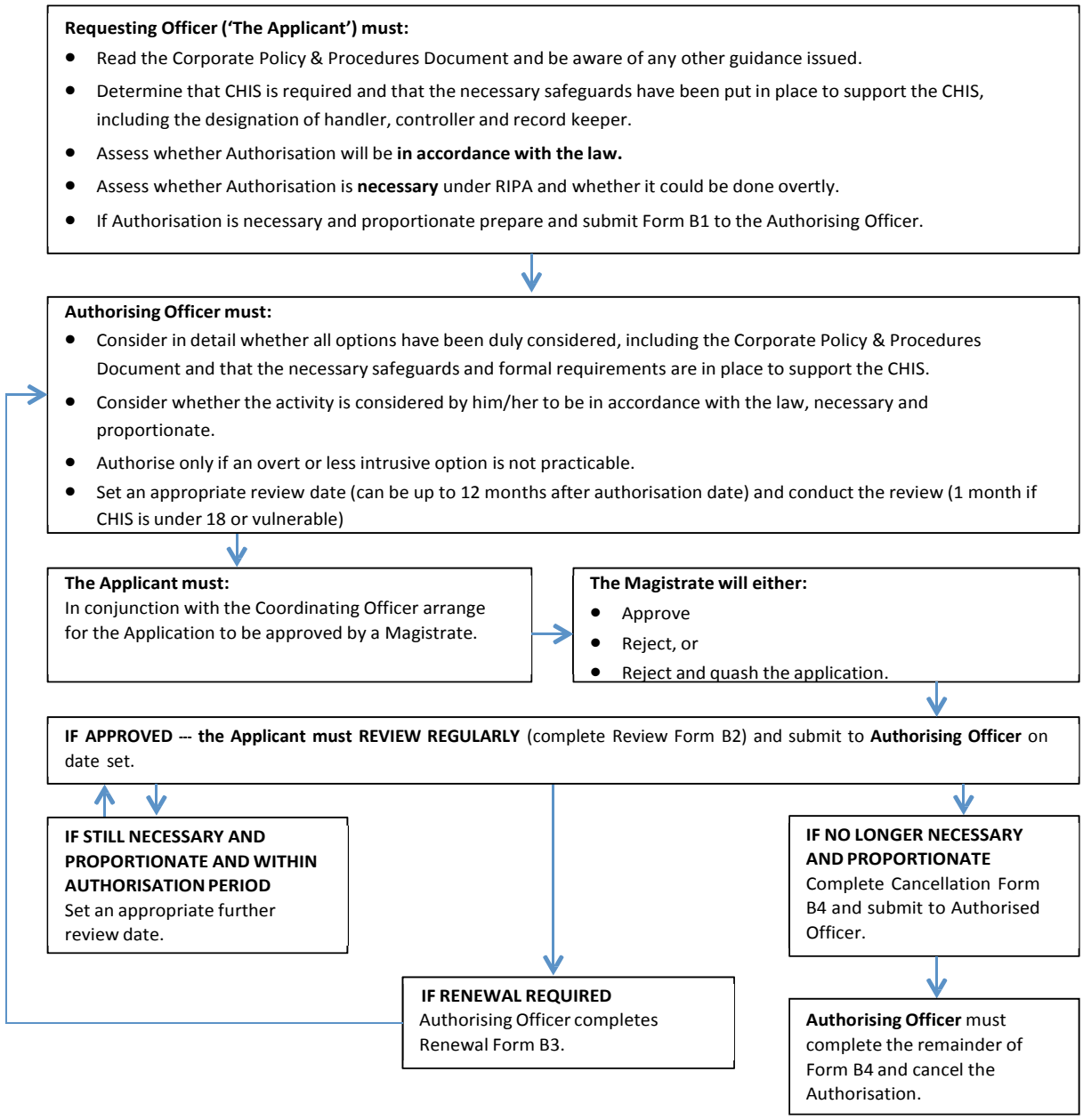
9.9 The Commissioner may also report, at any time, on any of their investigations and findings as they see fit. Public authorities may seek general advice from the Commissioner on any issue which falls within the Commissioner's statutory remit. The Commissioner may also produce whatever guidance they deem appropriate for public authorities on how to apply and use investigatory powers.

9.10 Further information about the Investigatory Powers Commissioner, their office and their work may be found at:www.ipco.org.uk

9.11 Oversight of public authorities in Northern Ireland, whose powers have been conferred by Order of the Northern Ireland Assembly, is a devolved matter.

APPENDIX E

CHIS FLOW CHART



ESSENTIAL

Send all ORIGINAL Authorised (and any rejected) Forms, Review, Renewals and Cancellations to the Coordinating Officer within 1 week of the relevant event.

If in doubt, consult the Senior Responsible Officer or the Coordinating Officer BEFORE any directed surveillance and/or CHIS are Authorised, Reviewed, Renewed, Cancelled, or rejected.

APPENDIX F

RIPA 'B' FORMS - CHIS

Form	Description
B1	Application for Authorisation of the use or conduct of a CHIS
B2	Review of Form B1
B3	Application for Renewal of Form B1
B4	Cancellation of Form B1

ALL FORMS MUST BE COMPLETED BY HAND

FORM B1 – APPLICATION FOR AUTHORISATION OF THE USE OR CONDUCT OF A COVERT HUMAN INTELLIGENCE SOURCE (CHIS)

PART II REGULATION OF INVESTIGATORY POWERS ACT 2000

SCARBOROUGH BOROUGH COUNCIL

STRICTLY PRIVATE AND CONFIDENTIAL

TO BE COMPLETED BY HAND

Unique Reference Number (URN)	
Subject of Surveillance (including full address)	

SECTION 1 (TO BE COMPLETED BY APPLICANT)

Name of Applicant		**Unit/Service**	
Full Address			
Contact Details			
How will the source be referred to (i.e. what will be his/her pseudonym or reference number)?			
What is the name, rank or position of the person within the relevant investigating authority who will have day to day responsibility for dealing with the source, including the source's security and welfare (often referred to as the Handler)?			

What is the name, rank or position of another person within the relevant investigating authority who will have general oversight of the use made of the source (often referred to as the	
Who will be responsible for retaining (in secure, strictly controlled conditions, with need-to-know access) the source's true identity, a record of the use made of the source and the particulars	
Investigation/Operation Name (if applicable)	
Investigating Officer (if person other than the Applicant)	

Details of Application

1. Give name and job title of Authorising Officer
2. Describe the purpose of the specific operation or investigation.
3. Describe in detail the purpose for which the source will be tasked or used.

4.	**Describe in detail the proposed covert conduct of the source or <u>how</u> the source is to be used**
5.	**Explain why the conduct or use of the source is NECESSARY in this particular case:**
6.	**Supply details of any potential COLLATERAL INTRUSION and why the intrusion is unavoidable: (Also describe precautions to MINIMISE collateral intrusion)**
7.	**Are there any particular sensitivities in the local community where the source is to be used? Are similar activities being undertaken by other public authorities that could impact on the deployment of the source?**

8. Provide an assessment of the risk to the source in carrying out the proposed conduct
9. Explain <u>why</u> this conduct or use of the source is PROPORTIONATE to what it seeks to achieve. How intrusive might it be on the subject(s) of surveillance or on others? How is this intrusion outweighed by the need for a source in operational terms, and could the evidence be obtained by any other means?
10. Confidential information (e.g. confidential legal privilege, personal information and journalistic material) INDICATE THE LIKELIHOOD OF ACQUIRING ANY CONFIDENTIAL INFORMATION
References for any other linked authorisations:

11. Applicant's Details	
Name:	**Tel No:**
Job Title:	**Date:**
Signature:	

12. Anticipated Start Date and Time	
Date:	**Time:**

SECTION 2 (TO BE COMPLETED BY AUTHORISING OFFICER)

13. Authorising Officer's Statement **MUST spell out the "5 Ws" – Who; What; Where; When; Why and HOW** **THE AUTHORISATION SHOULD IDENTIFY THE PSEUDONYM OR REFERENCE NUMBER OF THE SOURCE, NOT THE TRUE IDENTITY.**
14. Explain <u>why</u> you believe the conduct or use of the source is necessary **Explain <u>why</u> you believe the conduct or use of the source to be proportionate to what is sought to be achieved by their engagement**
Why is it necessary? Why is it proportionate?
15. Confidential Information Authorisation. Supply details demonstrating compliance with Home Office Codes of Practice relating to this issue.

Expiry of Authorisation:	
Date of first review:	
Programme for subsequent reviews of this authorisation. Only complete this box if review dates after first review are known. If not, or inappropriate to set additional review dates, then leave blank.	

Authorising Officer	
Job Title	
Signature	
Date/Time Granted	
Date/Time Ends (12 month period unless juvenile CHIS)	

NB: The original copy of this form, once it has been authorised or rejected, must be sent to the Coordinating Officer within 1 week of the authorisation or rejection for placing in the Central Register.

FORM B2 – REVIEW OF A COVERT HUMAN INTELLIGENCE SOURCE (CHIS) AUTHORISATION

PART II REGULATION OF INVESTIGATORY POWERS ACT 2000

SCARBOROUGH BOROUGH COUNCIL

STRICTLY PRIVATE AND CONFIDENTIAL

TO BE COMPLETED BY HAND

Unique Reference Number (URN)	
Subject of Surveillance (including full address)	

SECTION 1 (TO BE COMPLETED BY APPLICANT)

Name of Applicant		**Unit/Service**	
Full Address			
Contact Details			
Pseudonym or reference number of source			
Investigation/Operation Name (if applicable)			
Operation Number			
Investigating Officer (if person other than the Applicant)			
Date of authorisation or last renewal			
Expiry date of authorisation or last renewal			
Review Number			

Details of Review

1. Review Number and Dates of any Previous Reviews	
Review Number	**Dates**

2. Summary of the investigation/operation to date, including what information has been obtained and the value of the information so far obtained

3. Detail the reasons why it is NECESSARY to continue using a Covert Human Intelligence Source

4. Explain how the proposed activity is still PROPORTIONATE to what it seeks to achieve

5. Detail any incidents of collateral intrusion and the likelihood of any further incidents of collateral intrusions occurring	
6. Give details of any confidential information acquired or accessed and the likelihood of acquiring confidential information	
7. Give details of the review of the risk assessment on the security and welfare of using the source	
8. Applicant's Details	
Name:	**Tel No:**
Job Title:	**Date:**
Signature:	

SECTION 2 (TO BE COMPLETED BY AUTHORISING OFFICER)

9. Authorising Officer's Comments, including whether or not the directed surveillance should continue

10. Authorising Officer's Statement **THE AUTHORISATION SHOULD IDENTIFY THE PSEUDONYM OR REFERENCE NUMBER OF THE SOURCE, NOT THE TRUE IDENTITY.**
I [hereby agree that the use or conduct of the source for the purpose of the investigation/operation as detailed above [should/should not] continue [until its next review/renewal][it should be cancelled immediately].

Authorising Officer	
Job Title	
Signature	
Date/Time	

11. Date of Next Review	

NB: The original copy of this form, once it has been authorised or rejected, must be sent to the Coordinating Officer within 1 week of the authorisation or rejection for placing in the Central Register.

FORM B3 – APPLICATION FOR RENEWAL OF A COVERT HUMAN INTELLIGENCE SOURCE (CHIS) AUTHORISATION
(Please attach the original authorisation)

PART II REGULATION OF INVESTIGATORY POWERS ACT 2000

SCARBOROUGH BOROUGH COUNCIL

STRICTLY PRIVATE AND CONFIDENTIAL

TO BE COMPLETED BY HAND

Unique Reference Number (URN)	
Subject of Surveillance (including full address)	

SECTION 1 (TO BE COMPLETED BY APPLICANT)

Name of Applicant		**Unit/Service**	
Full Address			
Contact Details			
Pseudonym or reference number of source			
Investigation/Operation Name (if applicable)			
Investigating Officer (if person other than the Applicant)			
Date of authorisation or last renewal			
Expiry date of authorisation or last renewal			
Review Number			

Details of Renewal

1. Renewal Number and Dates of any Previous Renewals	
Renewal Number	**Date**

2. Detail any significant changes to the information provided in the original authorisation, as it applies at the time of the renewal

3. Detail the reasons why it is NECESSARY to continue with the authorisation, including details of any tasking given to the source

4. Detail why the use or conduct of the source is still PROPORTIONATE to what it seeks to achieve

5. Detail the use made of the source in the period since the grant of authorisation or, as the case may be, latest renewal of the authorisation.	
6. List the tasks given to the source during that period and the information obtained from the conduct or use of the source	
7. Detail the results of regular reviews of the use of the source	
8. Give details of the review of the risk assessment on the security and welfare of using the source	
9. Applicant's Details	
Name:	**Tel No:**
Job Title:	**Date:**
Signature:	

SECTION 2 (TO BE COMPLETED BY AUTHORISING OFFICER)

10. Authorising Officer's Comments **<u>This box must be completed</u>**
11. Authorising Officer's Statement **THE AUTHORISATION SHOULD IDENTIFY THE PSEUDONYM OR REFERENCE NUMBER OF THE SOURCE, NOT THE TRUE IDENTITY**
I hereby [authorise] [reject] the renewal of the conduct/use of the source as detailed above. [The renewal of this authorisation will last for 12 months unless renewed in writing] [This authorisation will be reviewed frequently to assess the need for the authorisation to continue.]

Authorising Officer	
Job Title	
Signature	
Date/Time	

12. Date of First Review	
13. Date of Subsequent Reviews of this Authorisation	

NB: The original copy of this form, once it has been authorised or rejected, must be sent to the Coordinating Officer within 1 week of the authorisation or rejection for placing in the Central Register.

FORM B4 – APPLICATION FOR CANCELLATION OF A COVERT HUMAN INTELLIGENCE SOURCE (CHIS) AUTHORISATION

PART II REGULATION OF INVESTIGATORY POWERS ACT 2000

SCARBOROUGH BOROUGH COUNCIL

STRICTLY PRIVATE AND CONFIDENTIAL

TO BE COMPLETED BY HAND

Unique Reference Number (URN)	
Subject of Surveillance (including full address)	

SECTION 1 (TO BE COMPLETED BY APPLICANT)

Name of Applicant		**Unit/Service**	
Full Address			
Contact Details			
Pseudonym or reference number of source			
Investigation/Operation Name (if applicable)			
Investigating Officer (if person other than the Applicant)			
Date of authorisation or last renewal			
Expiry date of authorisation or last renewal			

Details of Cancellation

7. Explain the reasons for the Cancellation of the Authorisation

8. Explain the value of the source in the operation:

9. Applicant's Details	
Name:	**Tel No:**
Job Title:	**Date:**
Signature:	

SECTION 2 (TO BE COMPLETED BY AUTHORISING OFFICER)

10. Authorising Officer's Statement THE AUTHORISATION SHOULD IDENTIFY THE PSEUDONYM OR REFERENCE NUMBER OF THE SOURCE, NOT THE TRUE IDENTITY
I hereby authorise the cancellation of the use or conduct of the source as detailed above.

Authorising Officer	
Job Title	
Signature	
Date/Time	

11. Time and Date of when the Authorising Officer instructed the use of the source to cease			
Date:		**Time:**	

12. Authorisation cancelled	Date:	Time:

NB: The original copy of this form, once it has been authorised or rejected, must be sent to the Coordinating Officer within 1 week of the authorisation or rejection for placing in the Central Register.