APPENDIX 1

REGULATION OF INVESTIGATORY POWERS ACT 2000

POLICY & PROCEDURES

FEBRUARY 2022

TABLE OF CONTENTS

1. INTRODUCTION & PURPOSE

1.1 The Regulation of Investigatory Powers Act 2000 (RIPA) was introduced in order to provide the correct balance between an individuals right to privacy under the Human Rights Act 1998 and the proper use of data and surveillance by public authorities, such as the police and local councils, who are entrusted by law to carry out certain enforcement duties.

1.2 The Act identifies certain areas where carrying out these enforcement duties will inevitably conflict with individuals rights to privacy. The main areas which are of concern to the Council are :

- The use of directed surveillance;
- The use of covert human intelligence sources (CHIS); and
- The acquisition of communications data.

1.3 Some of the Council's activities will necessarily require surveillance as part of their enforcement functions. Examples include fraud investigations and environmental, planning and licensing enforcement. The use of a CHIS may also be required by some Councils in very rare circumstances. The Regulation of Investigatory Powers Act 2000 provides the statutory framework for the granting of authority to carry out surveillance.

1.4 The requirement to acquire communications data is also very unlikely but if necessary this will be dealt with via the SPoC service offered by the National Anti-Fraud Network (NAFN).

1.5 Where the Council is required to gather evidence using surveillance and/or covert human intelligence sources or acquire communications data, these measures must be subject to an authorisation, review and cancellation procedure to ensure that it is lawful. A crime threshold (see 2.1 below) applies only to the authorisation of directed surveillance under RIPA, not to the authorisation of the use of CHIS or acquisition of communications data. Authorisation can only be given effect once an order approving the authorisation or notice has been granted by a Justice of the Peace (JP). In addition, the Council must comply with the Codes of Practice issued by the Home Secretary in accordance with the Act.

1.6 As a responsible local authority, the Council wishes to ensure that no individual, whether an employee of the Council or otherwise, suffers as a result of a breach of any provision of RIPA. It is essential that all activities of this nature, whether they will lead to prosecution or not, are carried out in accordance with RIPA, the Codes of Practice and this policy. Investigations which are not authorised could leave the Council open to legal challenge by individuals who consider that there has been an intrusion of their privacy.

1.7 It is necessary to have a corporate policy in order to describe and record the way in which the Council complies with RIPA. The policy applies to:

- all employees ;
- elected members ; and
- third parties acting on the Council's behalf, including all contractors, consultants and agents.

1.8 Where covert surveillance activities are unlikely to result in the obtaining of *private information* about a person, or where there is a separate legal basis for such activities, neither the 2000 Act nor the Home Office Codes of Practice need apply.

2. DIRECTED SURVEILLANCE

2.1 The use of directed surveillance is subject to the requirements of RIPA. Directed surveillance is defined by the Act as covert (carried out in a manner calculated to ensure that persons subject to the surveillance are unaware it is taking place) but not intrusive (covert and carried out in relation to anything taking place on residential premises or in a private vehicle and involves the presence of an individual on the premises or vehicle or is carried out by a surveillance device), and is undertaken :

- for the purposes of a specific investigation or specific operation to prevent or detect criminal offences that are either punishable, whether on summary conviction or indictment, by a maximum term of at least 6 months' imprisonment **or** are related to the underage sale of alcohol and tobacco (the crime threshold);
- in such a manner as is likely to result in the obtaining of private information about a person (whether or not one specifically identified for the purposes of the investigation or operation) ; and
- otherwise than by way of an immediate response to events or circumstances the nature of which is such that it would not be reasonably practicable for an authorisation under Part II of the 2000 Act to be sought for the carrying out of the surveillance.

Private information includes any information relating to a person's private or family life including any aspect of a person's private or personal relationship with others, such as family and professional or business relationships. Information which is non-private may include publicly available information such as books, newspapers, journals, TV and radio broadcasts, newswires, web sites, mapping imagery, academic articles, conference proceedings, business reports, and more. Such information may also include commercially available data where a fee may be charged, and any data which is available on request or made available at a meeting to a member of the public.

Whilst a person may have a reduced expectation of privacy when in a public place, covert surveillance of that person's activities in public may still result in the obtaining of private information. Surveillance of publicly accessible areas

of the internet should be treated in a similar way, recognising that there may be an expectation of privacy over information which is on the internet, particularly where accessing information on social media websites.

2.2 The statutory RIPA Code of Practice on covert surveillance makes it clear that general observation activities (which may include monitoring of publicly accessible areas of the internet in circumstances where it is not part of a specific investigation or operation), observation at trouble 'hotspots', immediate response to events and overt use of CCTV are all techniques which **do not require RIPA authorisation**. An authorisation for directed surveillance is only appropriate for the purposes of a specific investigation or operation, insofar as that investigation or operation is necessary on the grounds specified in the 2000 Act when in performance of its 'core functions' ('specific public functions', undertaken by a particular public authority, in contrast to the 'ordinary functions' which are those undertaken by all authorities).

2.3 RIPA regulates the way in which the Council carries out directed surveillance via the *Covert Surveillance and Property Interference Code of Practice (August 2018)* and sets a legal framework for any conduct carried out in accordance with the Act. This version of the code reflects changes introduced by the Investigatory Powers Act 2016 ("the 2016 Act"), including the new oversight framework, establishing the Investigatory Powers Commissioner ("the Commissioner").

3. COVERT HUMAN INTELLIGENCE SOURCES (CHIS)

3.1 If the use and conduct of a CHIS is being considered, urgent advice should be sought from the Senior Responsible Officer for RIPA before embarking on such a process. The use of a Covert Human Intelligence Source (CHIS) is subject to the requirements of RIPA. A CHIS is defined by the Act as a person who establishes or maintains a personal or other relationship with another person for the covert purpose of facilitating anything that :

- covertly uses such a relationship to obtain information or to provide access to any information to another person; or
- covertly discloses information obtained by the use of such a relationship or as a consequence of the existence of such a relationship.

A relationship is used covertly if, and only if, it is conducted in a manner calculated to ensure that the person is unaware of its purpose. A relationship is used covertly, and information obtained is disclosed covertly, if and only if the relationship is used or the information is disclosed in a manner that is calculated to ensure that one of the parties to the relationship is unaware of the use or disclosure in question. Public authorities are not required to seek or obtain an authorisation just because one is available. The use or conduct of a CHIS, can be a particularly intrusive and high-risk covert technique, requiring dedicated and sufficient resources, oversight and management. Authorisation is therefore advisable where a public authority intends to task someone to act as a CHIS, or where it is believed an individual is acting in that capacity and it

is intended to obtain information from them accordingly. Unlike directed surveillance, which relates specifically to private information, authorisations for the use or conduct of a CHIS do not relate specifically to private information, but to the covert manipulation of a relationship to gain any information. The Council will not in the normal course of any directed surveillance activity, use covert human intelligence sources, however if there is a justifiable need, this will be authorised in accordance with RIPA and the Protection of Freedoms Act 2012.

3.2 Not all human source activity will meet the definition of a CHIS as 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 (public volunteers). If personal knowledge has been acquired by mere observation, the informant is not a CHIS, however if personal knowledge is acquired in the course of (or as a result of the existence of) a personal or other relationship, the informant is a CHIS. If a public authority acts on the information provided by such a person without taking reasonable steps to protect their safety, it may be in breach of its duty of care if the person suffers reprisals. Therefore an authorisation will be required if a relationship exists between the subject and the CHIS, even if specific information has not been sought by the public authority.

3.3 RIPA regulates the way in which the Council can utilise a CHIS via the *Covert Human Intelligence Sources Code of Practice (August 2018)* and sets a legal framework for any conduct carried out in accordance with the Act. This version of the code reflects changes introduced by the Investigatory Powers Act 2016 ("the 2016 Act"), including the new oversight framework, establishing the Investigatory Powers Commissioner ("the Commissioner").

4. ACQUISITION OF COMMUNICATIONS DATA

4.1 The Investigatory Powers Act 2016 (IPA) governs how we use the investigatory powers available to us. These powers provide for the lawful acquisition of communications data (CD) including the who, where, when, how and with whom of a communication but not the content (i.e. what was said). IPA groups CD into two categories:

- 'entity data' - this data is about entities or links between them and describes or identifies the entity but does not include information about individual events. Entities could be individuals, groups and objects (such as mobile phones or other communications devices);;
- 'events data' - events data identifies or describes events in relation to a telecommunication system which consist of one or more entities engaging in an activity at a specific point, or points, in time.

4.2 Local authorities must submit all their communication data applications, via the National Anti-Fraud Network (NAFN) for the consideration of Office for Communications Data Authorisations (OCDA). All applications must be

authorised by OCDA prior to any communications data being acquired on behalf of a Local Authority. Applicants within local authorities are therefore required to consult a National Anti-Fraud Network (NAFN) SPoC throughout the application process. The accredited SPoCs at NAFN will scrutinise the applications independently. They will provide advice to the local authority ensuring it acts in an informed and lawful manner. The SPoC is an individual trained to facilitate the lawful acquisition of communications data and effective co-operation between a public authority, the OCDA and telecommunications operators and postal operators. Section 60A of the Act provides for the independent authorisation of communications data requests by the IPC. The OCDA performs this function on behalf of the IPC. An authorising officer in OCDA can authorise any request, for any purpose from any public authority. The introduction of the OCDA means the acquisition of communications data by local authority officers is no longer subject to judicial approval by a magistrate.

4.3 In addition to being considered by a NAFN SPoC, the local authority making the application must ensure someone of at least the rank of the senior responsible officer in the local authority is aware the application is being made before it is submitted to an authorising officer in OCDA. The local authority senior responsible officer must be satisfied that the officer(s) verifying the application is (are) of an appropriate rank and must inform NAFN of such nominations. NAFN will be responsible for submitting the application to OCDA on behalf of the local authority.

4.4 A local authority may not make an application that requires the processing or disclosure of internet connection records for any purpose.

4.5 If the acquisition of communications data is being considered, detailed guidance is provided in the Home Office Communications Data Code of Practice (November 2018). Advice should be sought from the Senior Responsible Officer for RIPA before embarking on such a process.

5. ONLINE COVERT ACTIVITY

5.1 The growth of the internet, and the extent of the information that is now available online, presents new opportunities for public authorities to view or gather information which may assist them in preventing or detecting crime or carrying out other statutory functions, as well as in understanding and engaging with the public they serve. It is important that public authorities are able to make full and lawful use of this information for their statutory purposes. Much of it can be accessed without the need for RIPA authorisation; use of the internet prior to an investigation should not normally engage privacy considerations. But if the study of an individual's online presence becomes persistent, or where material obtained from any check is to be extracted and recorded and may engage privacy considerations, RIPA authorisations may need to be considered. The viewing of open source activity is addressed by the Covert Surveillance and Property Interference Code of Practice (August

2018) paragraphs 3.10 to 3.17 and the Covert Human Intelligence Sources Code of Practice (August 2018) paragraphs 4.11 to 4.17.

5.2 The internet may be used for intelligence gathering and/or as a surveillance tool. Where online monitoring or investigation is conducted covertly for the purpose of a specific investigation or operation and is likely to result in the obtaining of private information about a person or group, an authorisation for directed surveillance should be considered. Where a person acting on behalf of the Council is intending to engage with others online without disclosing his or her identity, whether by publicly open websites such as an online news and social networking service, or more private exchanges such as e-messaging sites, a CHIS authorisation may be needed. This would include:

- An investigator using the internet to engage with a subject of interest at the start of an operation, in order to ascertain information or facilitate a meeting in person;
- Directing a member of the public (such as a CHIS) to use their own or another internet profile to establish or maintain a relationship with a subject of interest for a covert purpose.

5.3 A CHIS authorisation will not always be appropriate or necessary for online investigation or research. Some websites require a user to register providing personal identifiers (such as name and phone number) before access to the site will be permitted. Where a member of a public authority sets up a false identity for this purpose, this does not in itself amount to establishing a relationship, and a CHIS authorisation would not immediately be required, though consideration should be given to the need for a directed surveillance authorisation if the conduct is likely to result in the acquisition of private information, and the other relevant criteria are met.

5.4 Where a website or social media account requires a minimal level of interaction, such as sending or receiving a friend request before access is permitted, this may not in itself amount to establishing a relationship. Equally, the use of electronic gestures such as “like” or “follow” to react to information posted by others online would not in itself constitute forming a relationship. However, it should be borne in mind that entering a website or responding on these terms may lead to further interaction with other users and a CHIS authorisation should be obtained if it is intended for an officer of a public authority or a CHIS to engage in such interaction to obtain, provide access to or disclose information. Where it is intended that more than one officer will share the same online persona, each officer should be clearly identifiable within the overarching authorisation for that operation, providing clear information about the conduct required of each officer and including risk assessments in relation to each officer involved.

5.5 In deciding whether online surveillance should be regarded as covert, consideration should be given to the likelihood of the subject(s) knowing that the surveillance is or may be taking place. Use of the internet itself may be considered as adopting a surveillance technique calculated to ensure that the subject is unaware of it, even if no further steps are taken to conceal the

activity. Conversely, if reasonable steps have been taken to inform the public or particular individuals that the surveillance is or may be taking place, this can be regarded as overt and a directed surveillance authorisation will not normally be available.

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

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

5.8 Whether a public authority interferes with a person's private life includes a consideration of the nature of the public authority's activity in relation to that information. Simple reconnaissance of such sites (i.e. preliminary examination with a view to establishing whether the site or its contents are of interest) is unlikely to interfere with a person's reasonably held expectation of privacy and therefore is not likely to require a directed surveillance authorisation. But where a public authority is systematically collecting and recording information about a particular person or group, a directed surveillance authorisation should be considered. These considerations apply regardless of when the information was shared online.

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

- Whether the investigation or research is directed towards an individual or organisation;
- Whether it is likely to result in obtaining private information about a person or group of people;
- Whether it is likely to involve visiting internet sites to build up an intelligence picture or profile;
- Whether the information obtained will be recorded and retained;
- Whether the information is likely to provide an observer with a pattern of lifestyle;

- Whether the information is being combined with other sources of information or intelligence, which amounts to information relating to a person's private life;
- Whether the investigation or research is part of an ongoing piece of work involving repeated viewing of the subject(s);
- Whether it is likely to involve identifying and recording information about third parties, such as friends and family members of the subject of interest, or information posted by third parties, that may include private information and therefore constitute collateral intrusion into the privacy of these third parties.

5.10 Internet searches carried out by a third party on behalf of the Council, or with the use of a search tool, may still require a directed surveillance authorisation.

6. AUTHORISATION

6.1 Under RIPA and the statutory Codes of Practice, directed surveillance and covert human intelligence sources should only be authorised if the authorising officer is satisfied that :

- the action is necessary (in a democratic society) on one or more of the grounds identified in the Codes of Practice ; and
- the surveillance is proportionate to what is sought to be achieved

A local authority who wishes to authorise the use of directed surveillance or CHIS under RIPA will need to obtain an order approving the grant or renewal of an authorisation or notice from a JP (a District Judge or lay magistrate) before it can take effect. If the JP is satisfied that the statutory tests have been met and that the use of the technique is necessary and proportionate he/she will issue an order approving the grant or renewal for the use of the technique as described in the application. This judicial approval mechanism is in addition to the existing authorisation process under the relevant parts of RIPA as outlined in the Codes of Practice. **The amendment means that local authorities are no longer able to orally authorise the use of RIPA techniques.** All authorisations must be made in writing and require JP approval. The authorisation cannot commence until this has been obtained.

In addition, local authorities can only authorise use of **directed surveillance** under RIPA to prevent or detect criminal offences that are either punishable, whether on summary conviction or indictment, by a maximum term of at least 6 months' imprisonment **or** are related to the underage sale of alcohol and tobacco (the crime threshold). Examples of cases where the offence being investigated attracts a maximum custodial sentence of six months or more could include more serious criminal damage, dangerous waste dumping and serious or serial fraud.

6.2 If during the investigation it becomes clear that the activity being investigated does not amount to a criminal offence or that it would be a less serious offence that does not meet the crime threshold the use of directed surveillance

should cease. If a directed surveillance authorisation is already in force it should be cancelled. When a relevant error has occurred, the Council must notify the Investigatory Powers Commissioner as soon as reasonably practicable, and no later than ten working days (or as agreed with the Commissioner) after it has been established by appropriate internal governance processes that a relevant error has occurred.

6.3 Local authorities **cannot** authorise directed surveillance for the purpose of preventing disorder unless this involves a criminal offence(s) which meets the crime threshold and may not authorise the use of directed surveillance under RIPA to investigate low-level offences which may include, for example, littering, dog control and fly-posting. However covert surveillance may be conducted under other legislation without the protection afforded by an authorisation under RIPA.

6.4 Local Authorities are **NOT** authorised to conduct **Intrusive Surveillance**.

6.5 Local Authorities have no statutory powers to interfere with private property. If any 'trespass' is being considered during the course of authorised surveillance, the matter should be referred to the Executive Director (People) and Monitoring Officer as a matter of urgency.

6.6 Full details of the procedures to be followed for directed surveillance and covert human intelligence sources including details of the Council's Authorising Officers and the completion of the required documents can be found in this Policy and Procedures document.

6.7 Authorisation procedures for the acquisition of communications data are referred to in Section 4 of this document.

7. RESPONSIBILITIES

7.1 The Council is committed to ensuring that any enforcement, investigation or other activity is carried out in accordance with the Regulation of Investigatory Powers Act 2000. To ensure compliance all relevant policies and procedures must comply fully with the Act and be fit for purpose. Policy and Procedures and subsequent revisions will be approved by elected members.

7.2 The Council accepts its responsibility to comply with any statutory Codes of Practice issued by the Home Secretary in accordance with the Act. The Codes of Practice, which are made mandatory by the Act, are reflected in the Council's RIPA 2000 Procedures.

7.3 In compliance with the Act, copies of the Codes of Practice will be available, for reference purposes, to members of the public and to all members of staff, elected members and third parties acting on behalf of the Council in any of the prescribed activities. All employees and members will be made aware of their duties and responsibilities under the Act.

7.4 The Council expects that all officers, members and third parties acting on behalf of the Council, to perform their duties in a manner which respects the rights of the individual in accordance with the Human Rights Act 1998.

7.5 The Council should ensure that their actions when handling private information obtained by means of covert surveillance or by means of the use or conduct of a CHIS comply with relevant legal frameworks and the CSPI and CHIS codes, so that any interference with privacy is justified in accordance with Article 8(2) of the European Convention on Human Rights. Compliance with these legal frameworks, including data protection requirements, will ensure that the handling of private information so obtained continues to be lawful, justified and strictly controlled, and is subject to robust and effective safeguards.

7.6 All material obtained under the authority of a covert surveillance or through the use or conduct of a CHIS must be handled in accordance with safeguards which the Council has implemented in line with the requirements of the CSPI and CHIS codes. Dissemination, copying and retention of material must be limited to the minimum necessary for authorised purposes.

7.7 The Council regards any unlawful breach of any provision of the Act by any employee of the Council as a disciplinary matter. Any employee who breaches this policy may be dealt with under the Council's disciplinary procedure.

7.8 The Council's Executive Director (Governance & Commisioning) and Monitoring Officer will be the Senior Responsible Officer (SRO) for RIPA responsible for ensuring that appropriate steps are taken within the authority to comply with the requirements of the Act. These will include, but not be limited to:

- ensuring the integrity of the process in place within the Council to authorise directed surveillance and the management of CHIS;
- ensuring compliance with Part II of the 2000 Act and with statutory codes of practice;
- oversight of the reporting of errors to the relevant oversight Commissioner and the identification of both the cause(s) of errors and the implementation of processes to minimise repetition of errors;
- engagement with the Commissioners and inspectors when they conduct their inspections;
- where necessary, overseeing the implementation of any post inspection action plans recommended or approved by a Commissioner;
- nominating officers who will be designated as authorising officers for the purposes of the Act and Codes of Practice and ensuring that they are of an appropriate standard in light of any recommendations in the inspection reports prepared by the Investigatory Powers Commissioner;
- ensuring that sufficient resources will be allocated to support the process ;
- producing and maintaining corporate RIPA 2000 procedures and documentation based upon each of the statutory Codes of Practice as necessary ;

- ensuring, by means of risk assessment, that activities which may be covered by the Act are subject to proper justification, authorisation, enactment and completion ;
- ensuring that where relevant, staff and members are adequately trained and regularly reminded of their duties and responsibilities in respect of the Act ;
- ensuring that any authorised activity undertaken is proportionate to the matter under investigation and is in accordance with Article 8 of the Human Rights Act 1998 - the right to respect for private and family life (subject to the restrictions prescribed, which must be prescribed by law, necessary in a democratic society and a proportionate measure) ;
- ensuring that elected members periodically review the authority's use of RIPA powers and that those powers are being used consistently within the policy and procedures;
- ensuring measures are in place to inform investigating and authorising officers of any changes to existing Codes of Practice, new Codes of Practice and relevant case law which may require changes in procedures ; and
- ensuring that a central register of all authorisations, renewals and terminations is maintained and used to monitor compliance with the Act, Codes of Practice, Council Policy and procedures.

7.9 The officer in charge of each authorised directed surveillance operation will be responsible for the conduct of the operation. All activities which are covered by RIPA must be carried out in accordance with the Act, the statutory Codes of Practice and the Council's approved policy and procedures.

8. DIRECTED SURVEILLANCE PROCEDURES

8.24 What reference documents are there?

8.1 **Who in the Council may authorise directed surveillance?**

The following officers have been duly trained and are designated as Authorising Officers:

- Chief Executive — Mr Andrew P Stokes
- Executive Director (Finance & Customer Services) — TBA
- Executive Director (Place) — Mr Neil Rodgers

Ideally the Authorising Officer should not be responsible for authorising their own activities, i.e. those operations or investigations in which they are directly involved or for which they have direct responsibility.

8.2 **What additional authorisation for directed surveillance is required?**

A local authority who wishes to authorise the use of directed surveillance under RIPA will need to obtain an order approving the grant or renewal of an authorisation or notice from a JP (a District Judge or lay magistrate) before it can take effect. If the JP is satisfied that the statutory tests have been met and that the use of the technique is necessary and proportionate he/she will issue an order approving the grant or renewal for the use of the technique as described in the application. This judicial approval mechanism is in addition to the existing authorisation process under the relevant parts of RIPA as outlined in the Codes of Practice.

8.3 **How is an application for the authorisation of directed surveillance made?**

An application for authorisation for Directed Surveillance must be in writing on the current Home Office form (available here https://www.gov.uk/government/publications/application-for-use-of-directed-surveillance). It should specify:

- the action to be authorised;
- the identities, where known, of those to be the subject of directed surveillance;
- an account of the investigation or operation and nature of the surveillance;
- the grounds on which the authorisation is sought (e.g. for the purpose of preventing or detecting crime or of preventing disorder);
- why the directed surveillance is considered to be necessary and proportionate to what it seeks to achieve (see 8.5 below);
- an explanation of the information which it is desired to obtain as a result of the authorisation;
- the potential for collateral intrusion, that is to say, interference with the privacy of persons other than the subjects of the surveillance, and an assessment of the risk of such intrusion or interference and why any intrusion is justified;

- the likelihood of acquiring any legally privileged or confidential material;

There should then be a record of whether authority was given or refused, by whom and the time and date.

8.4 What will the Authorising Officer have to consider?

The Authorising Officer must be satisfied that the authorisation is necessary in accordance with Section 28(3) of the 2000 Act for directed surveillance and Statutory Instrument 2003 Number 3171 and the Protection of Freedoms Act 2012:

- for the purpose of preventing or detecting criminal offences that are either punishable, whether on summary conviction or indictment, by a maximum term of at least 6 months' imprisonment **or** are related to the underage sale of alcohol and tobacco (the crime threshold).

Before authorising surveillance the authorising officer should also take into account the risk of intrusion into the privacy of persons other than those who are directly the subjects of the investigation or operation (collateral intrusion). Measures should be taken, wherever practicable, to avoid or minimise unnecessary intrusion into the privacy of those who are not the intended subjects of the surveillance activity. Where such collateral intrusion is unavoidable, the activities may still be authorised, provided this intrusion is considered proportionate to what is sought to be achieved. An application for an authorisation should include an assessment of the risk of any collateral intrusion including the likelihood that any equipment or software deployed may cause intrusion on persons or property other than the subject(s) of the application. If an automated system such as an online search engine is used to obtain the information, the authorising officer should be made aware of its potential extent and limitations. The authorising officer should take this into account, when considering the proportionality of the surveillance.

The Authorising Officer must also believe that the surveillance is necessary and proportionate to what it seeks to achieve (see 8.5 below), and should set out, in their own words, why they are satisfied or why they believe the activity is necessary and proportionate. A bare assertion is insufficient.

8.5 What is meant by the term necessary and proportionate?

The person granting the authorisation must believe that the covert surveillance authorisation is necessary in the circumstances of the particular case for the statutory grounds detailed above. In order to be satisfied, the conduct that it is aimed to prevent or detect must be identified and clearly described, particularly if it is questionable whether serious crime criteria are met. Often missed is an explanation of why it is necessary to use the covert techniques requested.

Then, if the activities are necessary, an authorisation should demonstrate how an authorising officer has reached the conclusion that the activity is proportionate to what it seeks to achieve; including an explanation of the reasons why the method, tactic or technique proposed is not disproportionate.

Proportionality is a very important concept, and it means that any interference with a persons rights must be proportionate to the intended objective. This involves balancing the intrusiveness of the activity on the target and others who might be affected by it against the need for the activity in operational terms. The activity will not be proportionate if it is excessive in the circumstances of the case or if the information which is sought could reasonably be obtained by other less intrusive means. Thus where surveillance is proposed, that action must be designed to do no more than meet the objective in question. All such activity should be carefully managed to meet the objective in question and must not be arbitrary or unfair.

Proportionality is not only about balancing the effectiveness of covert methods over overt methods but of explaining why the particular covert method, technique or tactic is the least intrusive. It is insufficient to make a simple assertion or to say that the 'seriousness' of the crime justifies any or every method available. It may be unacceptable to advance lack of resources or a potential cost saving as sufficient ground to use technological solutions which can be more intrusive than a human being. This critical judgment can only properly be reached once all other aspects of an authorisation have been fully considered.

8.6 **What is the procedure for applying for judicial approval?**

Following approval by the authorising officer the Council will contact Her Majesty's Courts and Tribunals Service (HMCTS) administration team at the magistrates' court as soon as possible to request a hearing. The Council will then provide the JP with a copy of the original RIPA authorisation or notice and the supporting documents setting out the case. This forms the basis of the application to the JP and should contain all information that is relied upon. In addition, the local authority will provide the JP with a partially completed judicial application/order form.

The order section of this form will be completed by the JP and will be the official record of the JP's decision. The Council will need to obtain judicial approval for all initial RIPA authorisations/applications and renewals and the local authority will need to retain a copy of the judicial application/order form after it has been signed by the JP. There is no requirement for the JP to consider either cancellations or internal reviews.

On the rare occasions where out of hours access to a JP is required then it will be for the Council to make local arrangements with the relevant HMCTS legal staff who will require basic facts about the authorisation and the urgency. If the urgency is agreed, then arrangements will be made for a suitable JP to consider the application and attendance and evidence will be required. In

these cases the Council will need to provide two partially completed judicial application/order forms so that one can be retained by the JP. The Council should provide the court with a copy of the signed judicial application/order form the next working day.

No RIPA authority is required in immediate response to events or situations where it is not reasonably practicable to obtain it (for instance when criminal activity is observed during routine duties and officers conceal themselves to observe what is happening).

The hearing is a 'legal proceeding' and therefore local authority officers need to be formally designated to appear, be sworn in and present evidence or provide information as required by the JP. It is envisaged that the case investigator will be able to fulfil this role, however if practicable the Authorising Officer should be present to answer questions about their reasoning on necessity, proportionality, collateral intrusion and risk. If the Authorising Officer is not present, any comments made by the magistrate should be reported to them and recorded together with any action taken by the Authorising Officer to incorporate or address them. The hearing will be in private and heard by a single JP who will read and consider the RIPA authorisation or notice and the judicial application/order form. He/she may have questions to clarify points or require additional reassurance on particular matters.

8.7 **What will the Justice of the Peace consider and decide?**

The JP will consider whether he or she is satisfied that at the time the authorisation was granted or renewed or the notice was given or renewed, there were reasonable grounds for believing that the authorisation or notice was necessary and proportionate. They will also consider whether there continues to be reasonable grounds. In addition they must be satisfied that the person who granted the authorisation or gave the notice was an appropriate designated person within the local authority and the authorisation was made in accordance with any applicable legal restrictions, for example that the crime threshold for directed surveillance has been met.

The forms and supporting papers must by themselves make the case. It is not sufficient for the Council to provide oral evidence where this is not reflected or supported in the papers provided. If more information is required to determine whether the authorisation or notice has met the tests then the JP will refuse the authorisation. If an application is refused the Council may consider whether they can reapply, for example, if there was information to support the application which was available to the Council, but not included in the papers provided at the hearing.

Following their consideration of the case the JP will complete the order section of the judicial application/order form recording their decision. The JP may decide to:

- Approve the Grant or renewal of an authorisation or notice which will then take effect and the Council may proceed to use the technique in that particular case;
- Refuse to approve the grant or renewal of an authorisation or notice so the Council may **not** use the technique in that case. Where an application has been refused the Council may wish to consider the reasons for that refusal. For example, a technical error in the form may be remedied without the Council going through the internal authorisation process again. The Council may then wish to reapply for judicial approval once those steps have been taken;
- Refuse to approve the grant or renewal and quash the authorisation or notice. The court must not exercise its power to quash the authorisation or notice unless the Council has had at least 2 business days from the date of the refusal in which to make representations.

There is no complaint route for a judicial decision unless it was made in bad faith. A local authority may only appeal a JP decision on a point of law by judicial review.

8.8 **How long will the authorisation last?**

The written authorisation will cease to have effect (unless renewed or cancelled) at the end of a period of 3 months beginning with the date on which it took effect and expiring at 23:59 hours the day preceding.

8.9 **Can the Council carry out surveillance with other organisations?**

Any person granting or applying for an *authorisation* will also need to be aware of particular sensitivities in the local community where the surveillance is taking place and of any similar activities being undertaken by other *public authorities* which could impact on the deployment of surveillance. It is therefore recommended that where an *authorising officer* from a *public authority* considers that conflicts might arise they should consult a senior *officer* within the police force area in which the investigation or operation is to take place. Where possible, the Council should seek to avoid duplication of authorisations as part of a single investigation or operation. For example, where the Council is conducting directed surveillance as part of a joint operation, only one authorisation is required. The tasking or lead organisation should normally obtain or provide the authorisation under Part II of the 2000 Act. For example, where surveillance is carried out by the Council on behalf of HMRC, authorisations would usually be sought by HMRC and granted by their authorising officer.

In some circumstances it may be appropriate or necessary for a public authority to work with third parties who are not themselves a public authority (such as an individual, company or non-governmental organisation) to assist with an investigation. Where that third party is acting in partnership with or under the direction of a public authority, then they are acting as an agent of

that authority and any activities that third party conducts which meet the 2000 Act definitions of directed surveillance should be considered for authorisation under those Acts by the public authority on whose behalf that activity is being undertaken. Similarly, a surveillance authorisation should also be considered where the public authority is aware that a third party (that is not a public authority) is independently conducting surveillance and the public authority intends to make use of any suitable material obtained by the third party for the purposes of a specific investigation being undertaken by that public authority.

8.10 **When should reviews take place?**

There must be regular reviews of any authorisations given and the records of these reviews must be in writing and authorised by the Authorising Officer on the current Home Office form (available here https://www.gov.uk/government/publications/review-of-use-of-directed-surveillance). Any proposed or unforeseen changes to the *nature* or extent of the surveillance operation that may result in the further or greater intrusion into the private life of any person should also be brought to the attention of the *authorising officer* by means of a review. Where a directed surveillance *authorisation* provides for the surveillance of unidentified individuals whose identity is later established, the terms of the *authorisation* should be refined at a review to include the identity of these individuals. The frequency of reviews should be considered at the outset by the authorising officer as is considered necessary and practicable. Particular attention is drawn to the need to review authorisations frequently where the surveillance involves a high level of intrusion into private life or significant collateral intrusion, or confidential information is likely to be obtained. The results of a review should be recorded on the central record of authorisations and should be retained for at least three years.

8.11 **Can an authorisation be renewed?**

If at any time before an authorisation ceased to have effect, the Authorising Officer considers it necessary for the authorisation to continue for the same purpose for which it was given, then he/she may request renewal of the authorisation by a JP in writing on the current Home Office form (available here https://www.gov.uk/government/publications/renewal-form-for-directed-surveillance).

Applications for renewals should not be made until shortly before the original authorisation period is due to expire but must take account of factors which may delay the renewal process (e.g. intervening weekends or the availability of the Council's authorising officer and a JP to consider the application). A renewal must be authorised prior to the expiry of the original authorisation, but it runs from the expiry date and time of that original authorisation. The renewal will normally be for 3 months and authorisations may be renewed more than once if still considered necessary and proportionate and approved by the JP.

The renewal should be kept/recorded as part of the central record of authorisations. The request for a renewal of an authorisation should record:

- whether this is the first renewal, or on how many occasions it has been renewed;
- the same information as outlined for an original application;
- details of any significant difference in the information given in the previous authorisation;
- the reasons why it is necessary to continue with the surveillance;
- the content and value to the investigation or operation of the information so far obtained by the surveillance;
- whether any privileged material or confidential information was obtained as a result of activity undertaken under the authorisation, to which the safeguards in chapter 9 of the CSPI code should apply;
- the results of regular reviews of the investigation or operation;
- an estimate of the length of time the surveillance will continue to be necessary.

8.12 **Can or should an authorisation be revoked?**

The Authorising Officer who granted or last renewed the authorisation must cancel it if he/she is satisfied that the directed surveillance no longer meets the criteria for authorisation. Those acting under an authorisation must keep their authorisations under review and notify the authorising officer if they consider that the authorisation is no longer necessary or proportionate, and so should therefore be cancelled. Cancellation of directed surveillance must be in writing on the current Home Office form (available here https://www.gov.uk/government/publications/cancellation-of-use-of-directed-surveillance-form) and the date and time when such an instruction was given should be recorded in the central record of authorisations. When cancelling an authorisation, the authorising officer should record on the form:

- the date and times (if at all) that surveillance took place and the order to cease the activity was made;
- the reason for cancellation;
- ensure that surveillance equipment has been removed and returned;
- provide directions for the management of the product;
- ensure that detail of property interfered with, or persons subjected to surveillance since the last review or renewal is properly recorded;
- record the value of the surveillance or interference (i.e. whether the objectives as set in the authorisation were met).

As soon as a decision is taken to cease surveillance, an instruction must be given to those involved in the operation to stop all surveillance of the subject(s). The date on which that instruction is given should also be recorded.

8.13 **What is legally privileged material and other confidential material?**

Confidential material is anything:

- which is subject to legal privilege, for example, communications between legal advisers and their clients. Legal privilege does not apply to communications or items held, or oral communications made, with the intention of furthering a criminal purpose (whether the lawyer is acting unwittingly or culpably). Legally privileged communications will lose their protection if the professional legal adviser is intending to hold or use them for a criminal purpose. But privilege is not lost if a professional legal adviser is properly advising a person who is suspected of having committed a criminal offence.
- which is confidential personal information, for example information about someone's health or spiritual counselling or other assistance given or to be given to them;
- which is confidential constituent information, for example information about private constituency matters discussed between a Member of Parliament and a constituent;
- which is confidential journalistic material (this includes related communications), that is, material obtained or acquired for the purposes of journalism and held subject to an undertaking to hold it in confidence.

8.14 **How can knowledge of matters subject to legal privilege be obtained?**

Directed surveillance that is carried out in relation to anything taking place on so much of any premises specified in article 3(2) of the RIPA (Extension of Authorisation Provisions: Legal Consultations) Order 2010 as is, at any time during the surveillance, used for the purposes of 'legal consultations' shall be treated for the purposes of Part II of the 2000 Act as intrusive surveillance and cannot therefore be conducted by the Council.

Where directed surveillance is **likely or intended** to result in the acquisition of knowledge of matters subject to legal privilege, an authorisation shall only be granted or approved if the authorising officer is satisfied that there are exceptional and compelling circumstances that make the authorisation necessary:

- Where the surveillance is **not intended** to result in the acquisition of knowledge of matters subject to legal privilege, such exceptional and compelling circumstances may arise in the interests of national security or the economic well-being of the UK, or for the purpose of preventing or detecting serious crime;
- Where the surveillance **is intended** to result in the acquisition of knowledge of matters subject to legal privilege, such circumstances will arise only in a very restricted range of cases, such as where there is a threat to life or limb, or to national security, and the surveillance is reasonably regarded as likely to yield intelligence necessary to counter the threat.

8.15 **Are there any special rules for legally privileged material and other confidential material?**

Additional safeguards are required where the use of directed surveillance is likely to result in the acquisition of knowledge of matters subject to legal privilege:

- The Authorising Officer must be the Chief Executive or (in his absence) Executive Directors who must be satisfied that the proposed directed surveillance is proportionate to what is sought to be achieved;
- if directed surveillance is **not intended** to result in the acquisition of knowledge of matters subject to legal privilege, but it is **likely** that such knowledge will nevertheless be acquired during the operation, the application should identify all steps which will be taken to mitigate the risk of acquiring it;
- where matters subject to legal privilege via the use of directed surveillance are deliberately obtained, they may be used to counter the threat which led to it being obtained, but it will not be admissible in court;
- knowledge of matters subject to legal privilege, whether or not it is acquired deliberately, must be kept separate from law enforcement investigations or criminal prosecutions;
- In cases likely to result in obtaining knowledge of matters subject to legal privilege, the authorising officer or Investigatory Powers Commissioner may require regular reporting so as to be able to decide whether the authorisation should continue;
- where legally privileged material or other confidential material has been acquired and retained for purposes other than its destruction, it should be clearly marked as subject to legal privilege or as confidential and the matter should be reported to the relevant Commissioner or Inspector during their next inspection and the material should be made available to him if requested;
- confidential material should be destroyed as soon as its retention is no longer necessary;
- Where there is any doubt as to the handling and dissemination of confidential information or information which may be subject to legal privilege, advice should be sought from Legal Services before any further dissemination of the material takes place. Similar advice should also be sought where there is doubt over whether information is not subject to legal privilege due to the "in furtherance of a criminal purpose" exception;
- In those cases where items identified by Legal Services as being legally privileged have been acquired, this should be reported to the Commissioner as soon as reasonably practicable;
- In the course of an investigation, a public authority must not act on or further disseminate legally privileged items unless it has first informed the Investigatory Powers Commissioner that the items have been obtained, except in urgent circumstances;
- The retention of legally privileged information, or its dissemination to an outside body, should be accompanied by a clear warning that it is subject to legal privilege. It should be safeguarded by taking reasonable steps to

ensure there is no possibility of it becoming available, or its contents becoming known, to any person whose possession of it might prejudice any criminal or civil proceedings to which the information relates;
- Any dissemination of legally privileged material to an outside body should be notified to the relevant Commissioner or Inspector during their next inspection;
- Other confidential information, which can include both oral and written communications, 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.

8.16 **What records must be kept?**

Original documentation should be forwarded to the SRO for entry on the Central Record, oversight and secure storage. Practitioners should work from copy documents.

The following records must be kept centrally for a period of at least three years (up to five years desirable) from the ending of each authorisation. This information should be regularly updated whenever an authorisation is granted, renewed or cancelled and should be made available to the relevant Commissioner or an Inspector from the Investigatory Powers Commissioner's Office upon request :

- the type of authorisation;
- the date the authorisation was given;
- name and position of the authorising officer;
- the unique reference number (URN) of the investigation or operation;
- the title of the investigation or operation, including a brief description and names of subjects, if known;
- whether the urgency provisions were used, and if so why;
- details of attendances at the magistrates' court to include the date of attendances at court, the determining magistrate, the decision of the court and the time and date of that decision;
- the dates of any reviews;
- if the authorisation has been renewed, when it was renewed and who authorised the renewal, including the name and position of the authorising officer;
- whether the investigation or operation is likely to result in obtaining confidential information as defined in the code of practice;
- whether the authorisation was granted by an individual directly involved in the investigation;
- the date the authorisation was cancelled;
- where any application is refused, the grounds for refusal as given by the issuing authority or Judicial Commissioner;
- a record of whether, following a refusal of any application by a Judicial Commissioner, there is an appeal to the Investigatory Powers Commissioner;

- where there is such an appeal and the Investigatory Powers Commissioner also refuses the issuing of an application, the grounds for refusal given.

The following documentation should also be centrally retrievable for at least three years (up to five years desirable) from the ending of each authorisation:

- a copy of the application and a copy of the authorisation 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 to cease surveillance was given;
- the date and time when any other instruction was given by the authorising officer;
- a copy of the order approving or otherwise the grant or renewal of an authorisation from a Justice of the Peace (JP).

8.17 **Who keeps the record?**

The central register of records will be kept under the direction of the Council's SRO (Executive Director and Monitoring Officer) and held by the Council's Head of Audit.

8.18 **Will the material obtained be required as evidence in criminal proceedings?**

The Council must ensure that arrangements are in place for the secure handling, storage and destruction of material obtained through the use of directed surveillance in accordance with the Data Protection Act 2018. 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 further period, commensurate to any subsequent review.

8.19 **How should the material obtained be handled?**

Authorising officers, through their relevant Data Controller, must ensure compliance with the appropriate data protection requirements under the Data Protection Act 2018 and any relevant internal arrangements produced by individual authorities relating to the handling and storage of material.

The number of persons to whom any of the material acquired through covert surveillance is disclosed, and the extent of disclosure, should be limited to the minimum necessary for the authorised purpose(s). This obligation applies equally to disclosure to additional persons within the Council and to disclosure outside the Council. In the same way, only so much of the material may be

disclosed as the recipient needs; for example if a summary of the material will suffice, no more than that should be disclosed.

Material obtained through covert surveillance may only be copied to the extent necessary for the authorised purposes, and all copies, extracts and summaries of it, must be handled and stored securely, so as to minimise the risk of loss or theft. It must be held so as to be inaccessible to persons without the required level of security clearance (where applicable). This requirement to store such material securely applies to all those who are responsible for the handling of the material.

In particular, each public authority must apply the following protective security measures:

- physical security to protect any premises where the information may be stored or accessed;
- IT security to minimise the risk of unauthorised access to IT systems;
- an appropriate security clearance regime for personnel which is designed to provide assurance that those who have access to this material are reliable and trustworthy.

Information obtained through covert surveillance, and all copies, extracts and summaries which contain such material, should be scheduled for deletion or destruction and securely destroyed as soon as they are no longer needed for the authorised purpose(s). If such information is retained, it should be reviewed at appropriate intervals to confirm that the justification for its retention is still valid. In this context, destroying material means taking such steps as might be necessary to make access to the data impossible.

8.20 **What if surveillance activity has taken place without lawful authority?**

An error must be reported if it is a relevant error. Examples of relevant errors occurring would include circumstances where:

- Surveillance activity has taken place without lawful authority;
- There has been a failure to adhere to the safeguards set out in the relevant statutory provisions and Chapter 9 of the CSPI Code.

When a relevant error has occurred, the Council must notify the Investigatory Powers Commissioner as soon as reasonably practicable, and no later than ten working days (or as agreed with the Commissioner) after it has been established by appropriate internal governance processes that a relevant error has occurred. A full report must be sent to the Investigatory Powers Commissioner including information on the cause of the error; the amount of surveillance conducted and material obtained or disclosed; any unintended collateral intrusion; any analysis or action taken; whether any material has been retained or destroyed; and a summary of the steps taken to prevent recurrence. The Investigatory Powers Commissioner must inform a person of any relevant error relating to that person if the Commissioner considers that

the error is a serious error and that it is in the public interest for the person concerned to be informed of the error.

8.21 **Who is responsible for overseeing compliance with the 2000 Act?**

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 the CSPI code applies, and adherence to the practices and processes described in it. 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 Commissioner will have unfettered access to all locations, documentation and information systems as necessary to carry out their full functions and duties and all relevant persons using investigatory powers must provide all necessary assistance.

In addition, the Investigatory Powers Act establishes an independent Investigatory Powers Tribunal which has full powers to investigate, and decide upon, any case where a person complains that the conduct of the Council in exercising its powers whilst carrying out surveillance has infringed their human rights.

8.22 **Is the use of CCTV regulated by the Act?**

Guidance on the operation of overt CCTV cameras is provided in the Surveillance Camera Code of Practice issued under the Protection of Freedoms Act 2012. Although the provisions of the 2000 Act or of the covert surveillance code of practice do not normally cover the use of overt CCTV surveillance systems since members of the public are aware that such systems are in use by virtue of clearly visible signage, there may be occasions when the Council wishes to use overt CCTV systems for the purposes of a specific investigation or operation for the surveillance of a specific person or group of people which is likely to result in the obtaining of *private information* about a person (namely, a record of their movements and activities) and therefore falls properly within the definition of directed surveillance.. In such cases, the CCTV systems may be used covertly and authorisation for directed surveillance may be necessary.

8.23 **Are there any specific situations not requiring authorisation?**

The following specific activities constitute neither directed nor intrusive surveillance:

- the use of a recording device by a covert human intelligence source in respect of whom an appropriate use or conduct *authorisation* has been granted permitting them to record any information obtained in their presence;

- the recording, whether overt or covert, of an interview with a member of the public where it is made clear that the interview is entirely voluntary and that the interviewer is a *member* of a *public authority*;
- the covert recording of noise where: the recording is of decibels only or constitutes non-verbal noise (such as music, machinery or an alarm) or the recording of verbal content is made at a level which does not exceed that which can be heard from the street outside or adjoining property with the naked ear.

8.24 **What reference documents are there?**

The Council and those persons acting under Part II of the 2000 Act must have regard to the Codes of Practice issued under the Act. The Covert Surveillance and Property Interference Code of Practice is available here https://www.gov.uk/government/publications/covert-surveillance-and-covert-human-intelligence-sources-codes-of-practice .

Current Home Office prescribed RIPA forms for use by officers applying for authority, review, renewal and cancellation of Directed Surveillance are available here https://www.gov.uk/government/collections/ripa-forms--2 .

Home Office guidance on the judicial approval process for RIPA and the crime threshold for directed surveillance, including a flowchart outlining the procedure for application to a JP and judicial application / order form is available here https://www.gov.uk/government/publications/changes-to-local-authority-use-of-ripa .

Further Home Office guidance on the Regulation of Investigatory Powers Act is available here https://www.gov.uk/surveillance-and-counter-terrorism .

Further information on the work of the Investigatory Powers Commissioner's Office is available here https://www.ipco.org.uk/ .

Where fraud or corruption is suspected, officers are required to give due regard to the requirements of the Council's Counter Fraud and Corruption Strategy which is available on the Council's intranet.

If further guidance is required, please contact the Head of Audit on 01538 395695 or e-mail john.leak@staffsmoorlands.gov.uk .

9. RIPA 2000 COVERT HUMAN INTELLIGENCE SOURCE PROCEDURES

9.1 **Who in the Council may authorise use of a Covert Human Intelligence Source (CHIS)?**

If the use and conduct of a CHIS is being considered, urgent advice should be sought from the Senior Responsible Officer for RIPA before embarking on such a process.

The following officers have been duly trained and are designated as Authorising Officers by the Chief Executive:

- Chief Executive — Mr Andrew P Stokes
- Executive Director (Finance & Customer Services) — TBA
- Executive Director (Place) — Mr Neil Rodgers

Ideally the Authorising Officer should not be responsible for authorising a CHIS in connection with their own activities, i.e. those operations or investigations in which they are directly involved or for which they have direct responsibility, or where he/she would be the Controller or Handler.

9.2 **What additional authorisation for use of a CHIS is required?**

A local authority who wishes to authorise the use of a CHIS under RIPA will need to obtain an order approving the grant or renewal of an authorisation or notice from a JP (a District Judge or lay magistrate) before it can take effect. If the JP is satisfied that the statutory tests have been met and that the use of the technique is necessary and proportionate he/she will issue an order approving the grant or renewal for the use of the technique as described in the application. This judicial approval mechanism is in addition to the existing authorisation process under the relevant parts of RIPA as outlined in the Codes of Practice.

9.3 **How is an application for authorisation made?**

An application for authorisation for the use or conduct of a CHIS must be in writing on the current Home Office form (available here https://www.gov.uk/government/publications/application-for-the-use-of-covert-human-intelligence-sources-chis). It should specify:

- the details of the purpose for which the CHIS will be used;
- the identities, where known, of those to be the subject of the use or conduct of the CHIS;
- an account of the investigation or operation and details of what the CHIS will be asked to do;
- the grounds on which the authorisation is sought (e.g. for the purpose of preventing or detecting crime or of preventing disorder);
- why the use of CHIS is considered to be necessary and proportionate to what it seeks to achieve (see 9.5 below);
- an explanation of the information which it is desired to obtain as a result of the authorisation;

- details of the level of authority required;
- the potential for collateral intrusion, that is to say, interference with the privacy of persons other than the subjects of the investigation, and an assessment of the risk of such intrusion or interference and why any intrusion is justified;
- the likelihood of acquiring any legally privileged or confidential material and what that material might be;
- where the intention is to acquire knowledge of matters subject to legal privilege, the exceptional and compelling circumstances that make the authorisation necessary.`

There should then be a record of whether authority was given or refused, by whom, and the time and date.

9.4 **What will the Authorising Officer have to consider?**

The Authorising Officer must be satisfied that the authorisation is necessary in accordance with Section 29(3) of the 2000 Act for covert human intelligence sources and Statutory Instrument 2003 Number 3171 and the Protection of Freedoms Act 2012:

- for the purpose of preventing or detecting crime or of preventing disorder.

The Authorising Officer must also believe that:

- a risk assessment has been carried out to determine the risk to the CHIS of any tasking and the likely consequences should the role of the CHIS become known. The ongoing security and welfare of the CHIS, after the cancellation of the authorisation, should also be considered at the outset;
- the use of the CHIS is necessary and proportionate to what needs to be achieved (see 9.5 below). The authorising officer should set out, in their own words, why they are satisfied or why they believe the activity is necessary and proportionate. A bare assertion is insufficient;
- it is in compliance with relevant Articles of the European Convention on Human Rights, particularly Articles 6 and 8;
- satisfactory arrangements exist for the management of the CHIS;
- satisfactory arrangements exist for the statutory roles of handler and controller;
- there are arrangements for a person (the record keeper) to have responsibility for maintaining the source records in compliance with Statutory Instrument 2000 Number 2725.

9.5 **What is meant by the term necessary and proportionate?**

The person granting the authorisation must believe that the CHIS authorisation is necessary in the circumstances of the particular case for the statutory grounds detailed above. In order to be satisfied, the conduct that it is aimed to prevent or detect must be identified and clearly described. Often missed is an explanation of why it is necessary to use the covert techniques requested.

Then, if the use of the source is necessary, an authorisation should demonstrate how an authorising officer has reached the conclusion that the use of a source is proportionate to what it seeks to achieve; including an explanation of the reasons why the method, tactic or technique proposed is not disproportionate.

Proportionality is a very important concept, and it means that any interference with a persons rights must be proportionate to the intended objective. This involves balancing the intrusiveness of the use of the source on the target and others who might be affected by it against the need for the source to be used in operational terms. The use of a source will not be proportionate if it is excessive in the circumstances of the case or if the information which is sought could reasonably be obtained by other less intrusive means. Thus the use or conduct of the CHIS must be designed to do no more than meet the objective in question. All such activity should be carefully managed to meet the objective in question and must not be arbitrary or unfair.

Proportionality is not only about balancing the effectiveness of covert methods over overt methods but of explaining why the particular covert method, technique or tactic is the least intrusive. It is insufficient to make a simple assertion or to say that the 'seriousness' of the crime justifies any or every method available. It may be unacceptable to advance lack of resources or a potential cost saving as sufficient ground to use technological solutions which can be more intrusive than a human being. This critical judgment can only properly be reached once all other aspects of an authorisation have been fully considered.

9.6 **What is the procedure for applying for judicial approval?**

Following approval by the authorising officer the Council will contact Her Majesty's Courts and Tribunals Service (HMCTS) administration team at the magistrates' court as soon as possible to request a hearing. The Council will then provide the JP with a copy of the original RIPA authorisation or notice and the supporting documents setting out the case. This forms the basis of the application to the JP and should contain all information that is relied upon. In addition, the local authority will provide the JP with a partially completed judicial application/order form.

The order section of this form will be completed by the JP and will be the official record of the JP's decision. The Council will need to obtain judicial approval for all initial RIPA authorisations/applications and renewals and the local authority will need to retain a copy of the judicial application/order form after it has been signed by the JP. There is no requirement for the JP to consider either cancellations or internal reviews.

On the rare occasions where out of hours access to a JP is required then it will be for the Council to make local arrangements with the relevant HMCTS legal staff who will require basic facts about the authorisation and the urgency. If the

urgency is agreed, then arrangements will be made for a suitable JP to consider the application and attendance and evidence will be required. In these cases the Council will need to provide two partially completed judicial application/order forms so that one can be retained by the JP. The Council should provide the court with a copy of the signed judicial application/order form the next working day.

No RIPA authority is required in immediate response to events or situations where it is not reasonably practicable to obtain it (for instance when criminal activity is observed during routine duties and officers conceal themselves to observe what is happening).

The hearing is a 'legal proceeding' and therefore local authority officers need to be formally designated to appear, be sworn in and present evidence or provide information as required by the JP. It is envisaged that the case investigator will be able to fulfil this role. The hearing will be in private and heard by a single JP who will read and consider the RIPA authorisation or notice and the judicial application/order form. He/she may have questions to clarify points or require additional reassurance on particular matters.

9.7 **What will the Justice of the Peace consider and decide?**

The JP will consider whether he or she is satisfied that at the time the authorisation was granted or renewed or the notice was given or renewed, there were reasonable grounds for believing that the authorisation or notice was necessary and proportionate. They will also consider whether there continues to be reasonable grounds. In addition they must be satisfied that the person who granted the authorisation or gave the notice was an appropriate designated person within the local authority and the authorisation was made in accordance with any applicable legal restrictions.

The forms and supporting papers must by themselves make the case. It is not sufficient for the Council to provide oral evidence where this is not reflected or supported in the papers provided. If more information is required to determine whether the authorisation or notice has met the tests then the JP will refuse the authorisation. If an application is refused the Council may consider whether they can reapply, for example, if there was information to support the application which was available to the Council, but not included in the papers provided at the hearing.
Following their consideration of the case the JP will complete the order section of the judicial application/order form recording their decision. The JP may decide to:

- Approve the Grant or renewal of an authorisation or notice which will then take effect and the Council may proceed to use the technique in that particular case;
- Refuse to approve the grant or renewal of an authorisation or notice so the Council may **not** use the technique in that case. Where an application has been refused the Council may wish to consider the reasons for that refusal.

For example, a technical error in the form may be remedied without the Council going through the internal authorisation process again. The Council may then wish to reapply for judicial approval once those steps have been taken;

- Refuse to approve the grant or renewal and quash the authorisation or notice. The court must not exercise its power to quash the authorisation or notice unless the Council has had at least 2 business days from the date of the refusal in which to make representations.

There is no complaint route for a judicial decision unless it was made in bad faith. A local authority may only appeal a JP decision on a point of law by judicial review.

It is important that the CHIS is fully aware of the extent and limits of any conduct authorised and that those involved in the use of a CHIS are fully aware of the extent and limits of the authorisation in question.

9.8 **How long will the authorisation last?**

Except in relation to a juvenile CHIS and access to or disclosure of knowledge of matters subject to legal privilege, the written authorisation will cease to have effect (unless renewed) at the end of a period of 12 months beginning with the date on which it took effect and expiring at 23:59 hours the day preceding.

9.9 **Can the Council carry out the use or conduct of a CHIS with other organisations?**

Any person granting or applying for an authorisation will also need to be aware of any particular sensitivities in the local community where the CHIS is being used and of similar activities being undertaken by other public authorities which could have an impact on the deployment of the CHIS. Consideration should also be given to any adverse impact on community confidence or safety that may result from the use or conduct of a CHIS or use of information obtained from that CHIS. It is therefore recommended that where an authorising officer from a public authority considers that conflicts might arise they should, where possible, consult a senior officer within the police force area in which the CHIS is deployed. All public authorities, where possible, should consider consulting with other relevant public authorities to gauge community impact.

Where possible, the Council should seek to avoid duplication of authorisations as part of a single investigation or operation. For example, where the Council is conducting the use or conduct of a CHIS as part of a joint operation, only one authorisation is required. The tasking or lead organisation should normally obtain or provide the authorisation under Part II of the 2000 Act. For example, where the use or conduct of a CHIS is carried out by the Council on behalf of HMRC, authorisations would usually be sought by HMRC and granted by their authorising officer.

9.10 **When should reviews take place?**

There must be regular reviews of any authorisations given and the records of these reviews must be in writing and authorised by the Authorising Officer on the current Home Office form (available here https://www.gov.uk/government/publications/reviewing-the-use-of-covert-human-intelligence-sources-chis).The authorising officer should determine how often a review should take place which should be as frequently as is considered necessary and proportionate, but should not prevent reviews being conducted in response to changing circumstances. Particular attention should be given to the need to review authorisations frequently where they involve a high level of intrusion into private life or significant collateral intrusion, or the use of a CHIS may provide access to particularly sensitive information. The review should include the use made of the source during the period authorised, the tasks given to the source, the information obtained from the source and the reasons why executive action is not possible at this stage. The results of a review should be recorded on the central record of authorisations and the results of a review should be retained for at least five years.

Where the nature or extent of intrusion into the private or family life of any person becomes greater than that anticipated in the original authorisation, the authorising officer should immediately review the authorisation and reconsider the proportionality of the operation. This should be highlighted at the next renewal.

Where a CHIS authorisation provides for interference with the private and family life of initially unidentified individuals whose identity is later established, a new authorisation is not required provided the scope of the original authorisation envisaged interference with the private and family life of such individuals.

Any proposed changes to the nature of the CHIS operation (i.e. the activities involved) should immediately be brought to the attention of the authorising officer. The authorising officer should consider whether the proposed changes are within the scope of the existing authorisation and whether they are proportionate (bearing in mind any extra interference with private or family life or collateral intrusion), before approving or rejecting them. Any such changes should be highlighted at the next renewal.

9.11 **Can an authorisation be renewed?**

If at any time before an authorisation ceased to have effect, the Authorising Officer considers it necessary for the authorisation to continue for the same purpose for which it was given, then he/she may request renewal of the authorisation by a JP in writing on the current Home Office form (available here https://www.gov.uk/government/publications/renewal-of-authorisation-to-use-covert-human-intelligence-sources). Applications for renewals should not be made until shortly before the original authorisation period is due to expire but must take account of factors which may delay the renewal process (e.g.

intervening weekends or the availability of the Council's authorising officer and a JP to consider the application). A renewal must be authorised prior to the expiry of the original authorisation, but it runs from the expiry date and time of that original authorisation.

The renewal will normally be for 12 months and authorisations may be renewed more than once if still considered necessary and proportionate and approved by the JP. The renewal should be kept/recorded as part of the central record of authorisations. The request for a renewal of an authorisation should record:

- whether this is the first renewal, or on how many occasions it has been renewed;
- the same information as outlined for an original application;
- details of any significant difference in the information given in the previous authorisation;
- the reasons why it is necessary to continue with the CHIS;
- the use made of the CHIS in the period since the grant or, as the case may be, latest renewal of the authorisation;
- the tasks given to the CHIS during that period and the information obtained from the conduct or use of the CHIS;
- the results of regular reviews of the use of the CHIS.

9.12 **Can or should an authorisation be revoked?**

The Authorising Officer who granted or last renewed the authorisation must cancel it if he/she is satisfied that the use of the CHIS no longer meets the criteria for authorisation or that satisfactory arrangements for the CHIS's case no longer exist. Cancellation of the use of the CHIS must be in writing on the current Home Office form (available here https://www.gov.uk/government/publications/cancellation-of-covert-human-intelligence-sources-chis) and the date and time when such an instruction was given should be recorded in the central record of authorisations.

As soon as a decision is taken to cease the operation, an instruction must be given to those involved in the operation to stop using the CHIS. The date on which that instruction is given should also be recorded.

Where necessary, the safety and welfare of the CHIS should continue to be taken into account after the authorisation has been cancelled and risk assessments maintained. The authorising officer will wish to satisfy themselves that all welfare matters are addressed, and should make appropriate comment in their written commentary.

9.13 **What management arrangements should be in place for the Covert Human Intelligence Source?**

The following persons must be nominated in relation to each CHIS:

- A Handler - this person must be an officer of the Council (usually of a position below that of the authorising officer) and that person will have day to day responsibility for dealing with the CHIS, recording the information supplied by the CHIS and for monitoring the CHIS's security and welfare;
- A Controller - this person must be an officer of the Council and that person will have a general oversight of the use made of the CHIS;
- A Record Keeper - this person must be an officer of the Council who is given the responsibility for maintaining a record of the use made of the CHIS (usually the handler).

The Handler will need to explain to the CHIS what he or she must do. For example, the CHIS may be an environmental health officer who is asked to undertake a test purchase of items which are unfit for consumption.

It is not the intention that authorisations be drawn so narrowly that a separate authorisation is required each time the Handler asks the CHIS to do something. Rather, an authorisation might cover, in broad terms, the nature of the CHIS's task. If this changes, then a new authorisation may need to be sought.

When unforeseen action occurs, it must be recorded as soon as practicable after the event and, if the existing authorisation is insufficient, the existing authorisation must be updated and reauthorised (for minor amendments) or a new authorisation should be obtained before any further such action is carried out. Similarly where it is intended to task a source in a new way or significantly greater way than previously identified, the Handler or Controller must refer the proposed tasking to the authorising officer, who should consider whether a separate authorisation is required. This should be done in advance of any tasking and the details of such referrals must be recorded.

The day to day contact with the CHIS is to be conducted by the Handler. Some arrangements may be made in direct response to information provided by the CHIS on the occasion of his or her meeting with the Handler.

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 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.

Steps should be taken to protect the safety and welfare of the CHIS, when carrying out actions in relation to an authorisation, and to others who may be affected by the actions of a CHIS. 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 action and the likely consequences should the role of the CHIS become known to the subject of the investigation or those involved in the activity which is being investigated. The

ongoing security and welfare of the CHIS after the cancellation of the authorisation should also be considered at the outset.

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

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

Where deemed appropriate, the Controller must ensure that the information is considered by the Authorising Officer, and a decision taken on whether or not to allow the authorisation to continue.

9.14 **Can a juvenile be a Covert Human Intelligence Source?**

A juvenile is a person under the age of 18. Special safeguards apply to the authorisation where the CHIS would be a juvenile.

Authorisations should not be granted unless:

- a risk assessment has been undertaken as part of the application, covering the physical dangers and the psychological aspects of the use of the juvenile;
- the risk assessment has been considered by the Authorising Officer and he or she is satisfied that any risks identified in it have been properly explained;
- the Authorising Officer has given particular consideration as to whether the juvenile is to be asked to get information from a relative, guardian or any other person who has for the time being taken responsibility for the welfare of the juvenile. A juvenile under the age of 16 must never be authorised to give information against his or her parents or any person who has parental responsibility for him or her.

Authorisations should not be granted unless the Authorising Officer believes that management arrangements exist which will ensure that there will be at all times a person who has responsibility for ensuring that an appropriate adult will be present between any meetings between Council representatives and a CHIS under 16 years of age.

Authorisations for the use of a juvenile as a CHIS can be granted only by the Chief Executive or (in his absence) Executive Directors. The duration of such an authorisation is four months from the time of grant or renewal (instead of twelve months), and the authorisation should be subject to at least monthly review. For the purpose of these rules, the age test is applied at the time of the grant or renewal of the authorisation.

9.15 **What about vulnerable persons?**

Vulnerable persons are those who are 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. Only in the most exceptional circumstances should a vulnerable person be authorised to act as a CHIS and the authorisation must be given by the Chief Executive or (in his absence) Executive Directors.

9.16 **What type of things can a CHIS be asked to do?**

Once authorised a CHIS could be asked to obtain information, to provide access to information or to otherwise act incidentally for the benefit of the Council in the performance of its statutory enforcement and regulatory functions, if covered by the wording of the original authority. A CHIS, whether or not wearing or carrying a surveillance device, in residential premises or a private vehicle, does not require additional authorisation to record any activity taking place inside those premises or that vehicle which takes place in their presence.

A CHIS **must not** be asked to install a surveillance device nor **intercept** post or any other communications including those sent by telephone or email.

A CHIS **must not** be asked to do anything or not to do something which would involve the commission of a criminal offence by the CHIS, for example, a CHIS must not be asked to steal a document to get information.

9.17 **What is legally privileged material and other confidential material?**

Confidential material is anything:

- which is subject to legal privilege, for example, communications between legal advisers and their clients. Legal privilege does not apply to communications or items held, or oral communications made, with the intention of furthering a criminal purpose (whether the lawyer is acting unwittingly or culpably). Legally privileged communications will lose their protection if the professional legal adviser is intending to hold or use them for a criminal purpose. But privilege is not lost if a professional legal adviser is properly advising a person who is suspected of having committed a criminal offence.
- which is confidential personal information, for example information about someone's health or spiritual counselling or other assistance given or to be given to them;
- which is confidential constituent information, for example information about private constituency matters discussed between a Member of Parliament and a constituent;

- which is confidential journalistic material (this includes related communications), that is, material obtained or acquired for the purposes of journalism and held subject to an undertaking to hold it in confidence.

9.18 **Is an authorisation for acquiring matters subject to legal privilege different to other authorisations?**

The acquisition of matters subject to legal privilege (whether deliberate or otherwise) is subject to additional safeguards. These safeguards provide for three different circumstances where legally privileged items will or may be obtained. They are:

- where the Council seeks to grant or renew an authorisation for the use or conduct of a CHIS, in circumstances where it is intended to obtain, provide access to or disclose knowledge of matters subject to legal privilege, in which case the 2010 Legal Privilege Order will apply. Before an authorising officer grants or renews an authorisation to which the Order applies, they must give notice to and seek approval from a Judicial Commissioner (the approving officer). The authorising officer is prohibited from granting or renewing an authorisation until they have received confirmation in writing that the approving officer has approved the application. If the approving officer does not approve the application, the authorising officer may still grant an authorisation in respect of the use or conduct of the CHIS in question, but may not authorise the use or conduct of the CHIS to obtain, provide access to or disclose knowledge of matters subject to legal privilege. Approving officers may only approve, and authorising officers may only authorise, the use or conduct of CHIS to acquire knowledge of matters subject to legal privilege if they are satisfied that there are exceptional and compelling circumstances that make the authorisation necessary, for example, a threat to life a or limb or to national security, and it is likely to yield intelligence necessary to counter the threat.
- Where the use or conduct is not intended to result in the acquisition of knowledge of matters subject to legal privilege, but it is likely that such knowledge will nevertheless be acquired during the CHIS deployment the application should include, in addition to the reasons why the use or conduct is considered necessary, an assessment of how likely it is that information which is subject to legal privilege will be obtained. The Council should also confirm that any inadvertently obtained material that is subject to legal privilege will be treated in accordance with the safeguards set out in the CHIS code and that reasonable and appropriate steps will be taken to minimise access to the material that is subject to legal privilege.
- Where an application for an authorisation is made where the purpose or one of the purposes is to obtain items that, if they were not created or held with the intention of furthering a criminal purpose, would be subject to privilege and where the public authority considers that the items are likely to be created or held to further a criminal purpose, the application must include a statement to that effect and the reasons for believing that the items are likely to be created or held to further a criminal purpose. This includes applications to which the 2010 Legal Privilege Order would

otherwise apply (see 2(2)(b) of the Order). Information which may undermine the assessment that material is likely to be created or held to further a criminal purpose must also be included in the application to ensure the authorising officer can make an informed assessment about the nature of the material. The authorisation can only be approved where the authorising officer considers that the items are likely to be created or held with the intention of furthering a criminal purpose.

9.19 **What if a CHIS unintentionally obtains, provides access to or discloses knowledge of matters subject to legal privilege?**

Public authorities should make every effort to avoid their CHIS unintentionally obtaining, providing access to or disclosing knowledge of matters subject to legal privilege. If a public authority assesses that a CHIS may be exposed to such knowledge unintentionally, the public authority should task the CHIS in such a way that this possibility is reduced as far as possible. The reactive nature of the work of a CHIS, and the need for a CHIS to maintain cover, may make it necessary for a CHIS to engage in conduct which was not envisaged at the time the authorisation was granted, but which is incidental to that conduct, and may lead them to be exposed to matters subject to legal privilege. Such incidental conduct is regarded as properly authorised by the RIPA 2000 Act, even though it was not specified in the initial authorisation. This is likely to occur only in exceptional circumstances, such as where the obtaining of such knowledge is necessary to protect life and limb, including in relation to the CHIS, or national security, in circumstances that were not envisaged at the time the authorisation was granted.

When debriefing the CHIS, the public authority should make every effort to ensure that any knowledge of matters subject to legal privilege which the CHIS may have obtained is not disclosed to the public authority, unless there are exceptional and compelling circumstances that make such disclosure necessary. If, despite these steps, knowledge of matters subject to legal privilege is unintentionally disclosed to the public authority, the public authority in question should ensure that it is not used in law enforcement investigations or criminal prosecutions. Any unintentional obtaining of knowledge of matters subject to legal privilege by a public authority, together with a description of all steps taken in relation to that material, should be drawn to the attention of the Investigatory Powers Commissioner or inspectors supporting the work of the Commissioner during the next inspection (at which the material should be made available if requested).

If it becomes apparent that it will be necessary for the CHIS to continue to obtain, provide access to or disclose knowledge of matters subject to legal privilege, the initial authorisation should be cancelled and replaced by an authorisation that has been subject to the prior approval procedure, set out in the 2010 Legal Privilege Order, at the earliest reasonable opportunity.

9.20 **Are there any special rules for legally privileged material and other confidential material?**

Additional safeguards are required where the use or conduct of a CHIS may result in acquiring knowledge of legally privileged material or other confidential material. The following requirements apply:

- the Authorising Officer must be either the Chief Executive or (in his absence) Executive Directors who must be satisfied that the proposed directed surveillance is proportionate to what is sought to be achieved;
- an authorisation where it is intended to obtain, provide access to or disclose knowledge of matters subject to legal privilege is reduced from the usual 12 months to 3 months for any public authority);
- the application for authorisation must include an assessment of how likely it is that legally privileged material or other confidential material will be acquired;
- the application should clearly state whether the purpose (or one of the purposes) of the use or conduct of the CHIS is to obtain legally privileged material or other confidential material;
- where matters subject to legal privilege via the conduct of a CHIS are deliberately obtained, they may be used to counter the threat which led to it being obtained, but not for other purposes;
- knowledge of matters subject to legal privilege must be kept separate from law enforcement investigations or criminal prosecutions;
- In cases likely to result in obtaining knowledge of matters subject to legal privilege, the authorising officer or Investigatory Powers Commissioner may require regular reporting so as to be able to decide whether the authorisation should continue;
- where legally privileged material or other confidential material has been acquired and retained for purposes other than its destruction, it should be clearly marked as subject to legal privilege or as confidential and the matter should be reported to the relevant Commissioner or Inspector during their next inspection and the material should be made available to him if requested;
- confidential material should be destroyed as soon as its retention is no longer necessary;
- Where there is any doubt as to the handling and dissemination of confidential information or information which may be subject to legal privilege, advice should be sought from Legal Services before any further dissemination of the material takes place. Similar advice should also be sought where there is doubt over whether information is not subject to legal privilege due to the “in furtherance of a criminal purpose” exception.
- In those cases where items identified by Legal Services as being legally privileged have been acquired, this should be reported to the Commissioner as soon as reasonably practicable;

- In the course of an investigation, a public authority must not act on or further disseminate legally privileged items unless it has first informed the Investigatory Powers Commissioner that the items have been obtained, except in urgent circumstances;
- The retention of legally privileged information, or its dissemination to an outside body, should be accompanied by a clear warning that it is subject to legal privilege. It should be safeguarded by taking reasonable steps to ensure there is no possibility of it becoming available, or its contents becoming known, to any person whose possession of it might prejudice any criminal or civil proceedings to which the information relates.
- Any dissemination of legally privileged material to an outside body should be notified to the relevant Commissioner or Inspector during their next inspection.
- Other confidential information, which can include both oral and written communications, 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.

9.21 **What records must be kept?**

Original documentation should be forwarded to the SRO for entry on the Central Record, oversight and secure storage. Practitioners should work from copy documents. Matters relating to the true identity should be kept separate from operational documents.

The Central Record should be retained for a period of at least five years from the ending of the authorisations to which they relate and need only contain the name, code name, or unique identifying reference of the CHIS, the date the authorisation was granted, renewed or cancelled and an indication as to whether the activities were self-authorised. The following records must also be kept centrally for a period of at least five years from the ending of each authorisation. This information should be regularly updated whenever an authorisation is granted, renewed or cancelled and should be made available to the relevant Commissioner or an Inspector from the Investigatory Powers Commissioner's Office upon request:

- full details of the CHIS and the management arrangements for maintaining a record of the use made of the CHIS in order to preserve their confidentiality;
- a copy of the authorisation granted and, where relevant, a copy of any renewal of an authorisation granted;
- a copy of the original judicial application and renewal application / order form where relevant, after it has been approved and signed by the Justice of the Peace;
- any authorisation which was granted or renewed orally (in an urgent case) and the reason why the case was considered urgent;
- any risk assessment made in relation to the CHIS;
- the circumstances in which tasks were given to the CHIS;
- the value of the source to the Council;

- the reason why the person renewing an authorisation, considered it necessary to do so;
- the results of any reviews of the authorisation;
- the reasons, if any, for not renewing an authorisation;
- the reasons for cancelling an authorisation;
- the date and time when any instruction was given by the authorising officer to cease using a CHIS.

9.22 **What information should be kept about the CHIS?**

The following information should be available:

- the identity of the CHIS and the identity or identities used by the CHIS, where known;
- the means used within the Council of referring to the CHIS;
- any significant information connected with the security and welfare of the CHIS;
- any confirmation made by an Authorising Officer granting or renewing an authorisation for the conduct or use of a source, that the security and welfare of the CHIS has been considered and that any identified risks to the security and welfare of the CHIS have been properly explained to and understood by the CHIS;
- the date when, and the circumstances in which the CHIS was recruited;
- the authority for the related investigation or operation;
- the identities of the Controller, the Handler and the person monitoring the records of the CHIS;
- the period for which those responsibilities have been discharged by those persons;
- the tasks that are given to the CHIS and the demands made of them in relation to their activities as a CHIS;
- all contacts or communications between the CHIS and the Council or where the CHIS is a Council Officer, the Handler and the Controller;
- the information obtained by the Council by the conduct or use of the CHIS;
- in the case of a CHIS who is not an Officer of the Council, every payment, benefit or reward or every offer of a payment, benefit or reward that is made or provided by or on behalf of the Council in respect of the CHIS's activities for the benefit of the Council.

9.23 **Who may see the records?**

The records should be maintained in such a way as to preserve the confidentiality, or prevent disclosure of the identity of the CHIS, and the information provided by that CHIS.

9.24 **Who keeps the records?**

The detailed records outlined above will be kept by the person nominated as the record keeper for the CHIS. The central register of records will be kept

under the direction of the Council's SRO (Executive Director and Monitoring Officer) and held by the Council's Head of Audit.

9.25 **Will the material obtained be required as evidence in criminal proceedings?**

The Council must ensure that arrangements are in place for the secure handling, storage and destruction of material obtained through the use or conduct of a CHIS in accordance with the Data Protection Act 2018. Where the product of the use or conduct of a CHIS could be relevant to pending or future criminal or civil proceedings, it should be retained in accordance with applicable disclosure requirements.

9.26 **How should the material obtained be handled?**

Authorising officers, through their relevant Data Controller, must ensure compliance with the appropriate data protection requirements under the Data Protection Act 2018 and any relevant internal arrangements produced by individual authorities relating to the handling and storage of material.

The number of persons to whom any of the material acquired through use or conduct of a CHIS is disclosed, and the extent of disclosure, should be limited to the minimum necessary for the authorised purpose(s). This obligation applies equally to disclosure to additional persons within the Council and to disclosure outside the Council. In the same way, only so much of the material may be disclosed as the recipient needs; for example if a summary of the material will suffice, no more than that should be disclosed.

Material obtained through use or conduct of a CHIS may only be copied to the extent necessary for the authorised purposes, and all copies, extracts and summaries of it, must be handled and stored securely, so as to minimise the risk of loss or theft. It must be held so as to be inaccessible to persons without the required level of security clearance (where applicable). This requirement to store such material securely applies to all those who are responsible for the handling of the material.

In particular, each public authority must apply the following protective security measures:

- physical security to protect any premises where the information may be stored or accessed;
- IT security to minimise the risk of unauthorised access to IT systems;
- an appropriate security clearance regime for personnel which is designed to provide assurance that those who have access to this material are reliable and trustworthy.

Information obtained through use or conduct of a CHIS, and all copies, extracts and summaries which contain such material, should be scheduled for deletion or destruction and securely destroyed as soon as they are no longer

needed for the authorised purpose(s). If such information is retained, it should be reviewed at appropriate intervals to confirm that the justification for its retention is still valid. In this context, destroying material means taking such steps as might be necessary to make access to the data impossible

9.27 **What if covert human intelligence source activity activity has taken place without lawful authority?**

An error must be reported if it is a relevant error. Examples of relevant errors occurring would include circumstances where:

- covert human intelligence source activity has taken place without lawful authority;
- There has been a failure to adhere to the safeguards set out in the relevant statutory provisions and Chapter 8 of the CHIS Code.

When a relevant error has occurred, the Council must notify the Investigatory Powers Commissioner as soon as reasonably practicable, and no later than ten working days (or as agreed with the Commissioner) after it has been established by appropriate internal governance processes that a relevant error has occurred. A full report must be sent to the Investigatory Powers Commissioner including information on the cause of the error; the amount of covert human intelligence source activity conducted and material obtained or disclosed; any unintended collateral intrusion; any analysis or action taken; whether any material has been retained or destroyed; and a summary of the steps taken to prevent recurrence. The Investigatory Powers Commissioner must inform a person of any relevant error relating to that person if the Commissioner considers that the error is a serious error and that it is in the public interest for the person concerned to be informed of the error.

9.28 **Who is responsible for overseeing compliance with the 2000 Act?**

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 the CHIS code applies, and adherence to the practices and processes described in it. 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 Commissioner will have unfettered access to all locations, documentation and information systems as necessary to carry out their full functions and duties and all relevant persons using investigatory powers must provide all necessary assistance.

In addition, the Investigatory Powers Act establishes an independent Investigatory Powers Tribunal which has full powers to investigate, and decide upon, any case where a person complains that the conduct of the Council in exercising its powers has infringed their human rights.

9.29 **What about other types of informants?**

The 2000 Act does not apply to members of the public who volunteer information as part of their civic duties, or members of staff who report information in accordance with their contract of employment, or under the Councils Whistleblowing Policy.

9.30 **What reference documents are there?**

The Council and those persons acting under Part II of the 2000 Act must have regard to the Codes of Practice issued under the Act. The Covert Human Intelligence Sources Code of Practice is available here https://www.gov.uk/government/publications/covert-surveillance-and-covert-human-intelligence-sources-codes-of-practice .

Current Home Office prescribed RIPA forms for use by officers applying for authority, review, renewal and cancellation of the use of a Covert Human Intelligence Source are available here https://www.gov.uk/government/collections/ripa-forms--2 .

Home Office guidance on the judicial approval process for RIPA and the crime threshold for directed surveillance, including a flowchart outlining the procedure for application to a JP and judicial application / order form is available here https://www.gov.uk/government/publications/changes-to-local-authority-use-of-ripa .

Further Home Office guidance on the Regulation of Investigatory Powers Act is available here https://www.gov.uk/surveillance-and-counter-terrorism .

Further information on the work of the Investigatory Powers Commissioner's Office is available here https://www.ipco.org.uk/ .

Where fraud or corruption is suspected, officers are required to give due regard to the requirements of the Council's Counter Fraud and Corruption Strategy which is available on the Council's intranet.

If further guidance is required, please contact the Head of Audit on 01538 395695 or e-mail john.leak@staffsmoorlands.gov.uk .