HBC Corporate Surveillance Policy and Procedure

Last review date	**June 2022**
Next review date	**June 2023**
Policy Owner	**Executive Head for Internal Services**
Applicable	**All staff including those contractors acting on behalf of the Authority (i.e. an agent)**

CORPORATE SURVEILLANCE POLICY AND PROCEDURE

THE REGULATION OF INVESTIGATORY POWERS ACT 2000

CONTENTS

CORPORATE SURVEILLANCE POLICY

1.0 BACKGROUND

1.1 Summary

The Regulation of Investigatory Powers Act 2000 ('RIPA') brought into force the regulation of covert investigation by a number of bodies, including local authorities. Separate legislation (the Investigatory Powers Act 2016) (IPA) came into full effect on 11 June 2019 and is now the main legislation governing communications data. This document and the related procedure is intended to provide officers with guidance on the use of covert surveillance, Covert Human Intelligence Sources ('Sources') and the obtaining and disclosure of communications data under RIPA. Officers must take into account the Codes of Practice issued under RIPA (RIPA may be found at: www.legislation.gov.uk/ukpga/2000/23/contents and the Codes of Practice may be found at: www.gov.uk/government/collections/ripa-codes).

1.2 **Background**

The Human Rights Act 1998 requires the Council, and organisations working on its behalf, pursuant to Article 8 of the European Convention, to respect the private and family life of a citizen, his home and his correspondence. The European Convention did not, however, make this an absolute right, but a qualified right. Accordingly, in certain circumstances, the Council may interfere in the citizen's right mentioned above, if such interference is:

(a) in accordance with the law
(b) necessary (as defined in this document); and
(c) proportionate (as defined in this document).

In exceptional circumstances, Council Officers may engage in covert surveillance. RIPA provides a statutory mechanism for authorising certain types of surveillance. It seeks to ensure that any interference with an individual's right under Article 8 of the European Convention is necessary and proportionate. In doing so, RIPA seeks to ensure both the public interest and the human rights of individuals are suitably balanced.

If the correct procedures are not followed, evidence may be disallowed by the courts, a complaint of maladministration could be made to the Ombudsman. More particularly, a complaint could be made to the Investigatory Powers Tribunal, which is a judicial body, independent of government, which hears complaints about surveillance by public bodies. It is essential, therefore, that all involved with RIPA comply with this document and any further guidance that may be issued, from time to time, by the designated Senior Responsible Officer, this is assigned to the Executive Head for Internal Services.

Each officer of the Council with responsibilities for the conduct of investigations, shall, before carrying out any investigation involving RIPA, undertake

appropriate training to ensure that investigations and operations that he/she carries out will be conducted lawfully.

The Senior Responsible Officer's role is to ensure the integrity of the process within the Council and its compliance with RIPA; to have oversight of reporting of errors to the relevant oversight commissioner; responsibility for engagement with the IPCO (Investigatory Powers Commissioner's Office) when they conduct their inspections and where necessary, oversight of the implementation of any post-inspection action plan. The Senior Responsible Officer will also ensure that councillors have the opportunity to review the Council's use of RIPA. The record keeper for each authority will be the designated RIPA Coordinator.

This policy has been prepared to set out the relevant responsibilities and to ensure that any covert surveillance or the conduct and use of covert human intelligence sources is conducted by officers in a manner that will comply with the safeguards embodied in the Human Rights Act 1998 and RIPA. Pursuance of this policy will assist the Council if it is required at any time to demonstrate that it has acted lawfully.

1.3 Review

RIPA and this document are important for the effective and efficient operation of the Council's actions with regard to surveillance. This policy and its related procedure will, therefore be kept under yearly review by the Senior Responsible Officer and by the Council's Audit & Finance Committee. Authorising Officers must bring any suggestions for continuous improvement of this document to the attention of the Senior Responsible Officer at the earliest possible opportunity.

1.4 Scope

RIPA covers the authorisation of directed surveillance, the authorisation of sources. The authorisation of the obtaining of communications data is subject to provisions set out in IPA 2016. Communications data includes information relating to the use of a postal service or telecommunications system but does not include the contents of the communication itself, contents of e-mails or interaction with websites. An authorisation under RIPA will provide lawful authority for the investigating officer to carry out surveillance.

In terms of monitoring e-mails and internet usage, it is important to recognise the interplay and overlaps with the Council's e-mail and internet policies and guidance, the Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000 and the Data Protection Act 2018.

RIPA forms should be used where **relevant** and they will only be relevant where the **criteria** listed on the forms are fully met.

2. COVERT SURVEILLANCE PROCEDURE

2.1 Definition of Surveillance

Surveillance' includes:

- monitoring, observing or listening to persons, their movements, their conversations or their other activities or communication;
- recording anything monitored, observed or listened to in the course of surveillance; and
- surveillance by or with the assistance of a surveillance device.

Surveillance can be overt or covert.

2.2 Overt Surveillance

Most of the surveillance carried out will be done overtly – there will be nothing secretive, clandestine or hidden about it. In many cases, Officers will be going about Council business openly (e.g. a market inspector walking through markets).

Similarly, surveillance will be overt if the subject has been told it will happen (e.g. where a noisemaker is warned, usually in writing, that noise will be recorded if the noise continues)

2.3 Covert Surveillance

Covert surveillance as defined in section 26(9)(a) RIPA:

- "Surveillance is covert if, and only if, it is carried out in a manner that is calculated to ensure that persons who are subject to the surveillance are unaware that it is or may be taking place".

Covert Surveillance involves the systematic surveillance of an individual. The everyday investigatory and regulatory functions of a local authority will not usually involve covert surveillance.

2.4 Confidential Material

Particular care should be taken in cases where the subject of the investigation or operation might reasonably expect a high degree of privacy, or where confidential information is involved. Confidential information consists of matters subject to legal privilege, confidential personal information, confidential journalistic material and communications between an MP and a constituent.

Applications in which the surveillance is likely to result in the acquisition of confidential material will only be considered in exceptional and compelling circumstances with full regard to the proportionality issues this raises.

The Authorising Officer shall give the fullest consideration to any cases where the subject of the surveillance might reasonably expect a high degree of privacy, for instance in his or her home.

Where a likely consequence of surveillance would result in the acquisition of confidential material, the investigating officer must seek authorisation from the Chief Executive, or, in her absence, her authorised Deputy.

3. DIRECTED AND INTRUSIVE SURVEILLANCE

3.1 Directed Surveillance

Directed surveillance is surveillance which is covert, but not intrusive, and undertaken:

a) for the purposes of a specific investigation or specific operation;

b) 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

c) 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 RIPA to be sought for the carrying out of the surveillance.

Directed Surveillance is the type of surveillance with which Council Officers may be involved.

3.2 Intrusive Surveillance

Local authorities are not authorised to carry out intrusive surveillance. Only the police and certain law enforcement agencies may carry out intrusive surveillance. Council officers, or anyone on behalf of the Council, must not carry out intrusive surveillance.

That surveillance becomes intrusive if the covert surveillance:

a) is carried out by means of a surveillance device in relation to anything taking place on any residential premises or in any private vehicle; or

b) is carried out without that device being present on the premises or in the vehicle, is not intrusive unless the device is such that it consistently provides information of the same quality and detail as might be expected to be obtained from a device actually present on the premises or in the vehicle, or

c) is carried out in places ordinarily used for legal consultation, at a time when they are being used for such consultations.

Therefore directed surveillance turns into intrusive surveillance if it is carried out involving anything that occurs on residential premises or any private vehicle and involves the presence of someone on the premises or in the vehicle or is carried out by means of a surveillance device OR when directed surveillance is carried out in places ordinarily used for legal consultation, at a time when they are being used for such consultations.

For intrusive surveillance relating to residential premises or private vehicles, if any device used is not on the premises or in the vehicle, it is only intrusive surveillance if it consistently produces information of the same quality as if it were.

A local authority cannot authorise the fitting of trackers etc to private vehicles, such that it would constitute property interference (which, like intrusive surveillance, a Council cannot authorise). Commercial premises and vehicles are excluded from intrusive surveillance.

4. IDENTIFYING DIRECTED SURVEILLANCE

Ask yourself the following questions:

4.1 Is the surveillance covert?

Covert surveillance is any surveillance that is carried out in a manner calculated to ensure that the persons subject to the surveillance are unaware that it is or may be taking place. If your activities are not hidden from the subjects of your investigation, you are not within the RIPA framework at all. In many cases, Officers will be behaving in the same way as a normal member of the public (eg in the case of most test purchases), and/or will be going about Council business openly (eg a market inspector walking through markets).

Similarly, surveillance will be overt if the subject has been told it will happen (eg where a noisemaker is warned (preferably in writing) that noise will be recorded if the noise continues, or where an entertainment licence is issued subject to conditions, and the licensee is told that officers may visit without notice or identifying themselves to the owner/proprietor to check that conditions are being met.

It should be noted that if the same outcome can be achieved by overt means then those means need to be fully explored in the first instance. Covert surveillance must only be undertaken when there is no less invasive way of achieving the outcome.

4.2 Is the surveillance for the purposes of a specific investigation or a specific operation?

Although the provisions of the Act do not normally cover the use of overt CCTV surveillance systems, since members of the public are aware that such systems are in use, there may be occasions when public authorities use overt CCTV systems for the purposes of a specific investigation or operation. For example, if the CCTV cameras are targeting a particular known offender. In such cases, authorisation for directed surveillance may be necessary.

4.3 Is the surveillance in such a manner that is likely to result in the obtaining of private information about a person?

Private information includes any information relating to a person's private or family life. The concept of private information should be broadly interpreted to include an individual's private or personal relationship with others. It includes an individual's business and family relationships. Family life itself should be treated as extending beyond the formal relationships created by marriage.

4.4 Is the surveillance otherwise than by way of an immediate response to events or circumstances where it is not reasonably practicable to get authorisation?

Directed surveillance does not include covert surveillance carried out by way of an immediate response to events or circumstances which, by their very nature, could not have been foreseen. For example, a litter enforcement officer would not require an authorisation to conceal himself and observe a suspicious person that he came across in the course of his normal patrol.

However, if as a result of that immediate response, you undertake a specific investigation you will need authorisation.

5. COVERT HUMAN INTELLIGENCE SOURCES

5.1 Definition

A person is a source (CHIS) if:

a) he establishes or maintains a personal or other relationship with a person for the covert purpose of facilitating the doing of anything falling within paragraph (b) or (c);

b) he covertly uses such a relationship to obtain information or to provide access to any information to another person; or

c) he covertly discloses information obtained by the use of such a relationship or as a consequence of the existence of such a relationship.

A source may include those referred to as agents, informants, the Council's own officers or members of the public.

A purpose is covert, in relation to the establishment or maintenance of a personal or other relationship, if and only if, the relationship is conducted in a manner that is calculated to ensure that one of the parties to the relationship is unaware of the purpose.

A relationship is used covertly, and information obtained is disclosed covertly, if and only if it is used or 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.

The use of a source involves inducing, asking or assisting a person to engage in the conduct of a source, or to obtain information by means of the conduct of such a source.

This covers the use of professional witnesses to obtain information and evidence. For example, it will include professional witnesses retained by Housing to pose as tenants to obtain information and evidence against alleged nuisance perpetrators.

5.2 Specific matters relating to CHIS

In respect of Covert Human Intelligence Sources it is necessary under S29(5) RIPA that there are in force such arrangements as are necessary for ensuring:

(a) that there will at all times be a person holding an office, rank or position with the relevant investigatory authority who will have day to day responsibility for dealing with the CHIS on behalf of that authority and for the CHIS's security and welfare;

(b) that there will at all times be **another person** holding an office, rank or position with the relevant investigating authority who will have general oversight of the use made of the CHIS;

(c) that there will at all times be a person holding an office, rank or position with the relevant investigating authority who will have responsibility for maintaining a record of the use made of the CHIS

It should be noted that the roles of handler, controller and authoriser are discrete functions. If a Council officer is acting as CHIS, that person cannot play any part in the application or authorisation process. There must be an officer given direct day to day management of the CHIS to look after his/her needs and another officer in overall control of the use of the CHIS. A record must be made by a specified person of the use of the CHIS. Regulations have been made giving details of the type of particulars needed to be recorded. At the outset, a risk assessment is an essential first step in considering whether to use someone as a CHIS.

5.3 Test Purchases

Carrying out test purchases will not require the purchaser to establish a relationship with the supplier with the covert purpose of obtaining information and, therefore, the purchaser will not normally be a CHIS. For example, authorisation would not normally be required for test purchases carried out in the ordinary course of business (eg walking into a shop and purchasing a product over the counter). By contrast, developing a relationship with a person in the shop, to obtain information about the seller’s suppliers of an illegal product will require authorisation as a CHIS. Similarly, using mobile hidden recording devices or CCTV cameras to record what is going on in the shop will require authorisation as directed surveillance.

The Code of Practice states that the provisions of RIPA are not intended to apply in circumstances where members of the public volunteer information to the police or other authorities, as part of their normal civic duties, or to contact numbers set up to receive information (such as Crimestoppers, Customs Confidential, the Anti Terrorist Hotline, or the Security Service Public Telephone Number). Members of the public acting in this way would not generally be regarded as sources, so long as they provide information from their own observations.

However, asking a source to obtain information should not be used as the sole benchmark in seeking a CHIS authorisation. It is the activity of the CHIS in exploiting a relationship for a covert purpose which is ultimately authorised by the 2000 Act, whether or not that CHIS is asked to do so. It is possible therefore that a person will become engaged in the conduct of a CHIS without being induced, asked or assisting the person to engage in that conduct.

If the informant is a CHIS, he or she is a person to whom a duty of care is owed. If information provided by a CHIS is to be acted upon, that information must be independently corroborated before taking action.

An authorisation under RIPA will provide lawful authority for the use of a source.

6. INTERNET AND SOCIAL NETWORKING SITES

6.1 Use of Internet and social media

The Council may view or gather information which may assist it in preventing or detecting crime or carrying out other statutory functions, as well as in understanding and engaging with the public it serves. 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. This section of the policy is intended to assist officers in identifying when such authorisations may be appropriate.

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 an officer is intending to engage with others online without disclosing his or her identity, a CHIS authorisation may be needed.

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, where the Council has taken reasonable steps to inform the public or particular individuals that the surveillance is or may be taking place, the activity may be regarded as overt and a directed surveillance authorisation will not normally be necessary.

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.

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.

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.

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.

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

Officers using the internet for investigative purposes must not use their own personal devices (PC, laptop, tablet, smart phone etc.). It is important to bear in mind that all internet activity leaves a 'footprint'. Websites can routinely gather IP addresses and in some cases 'data trawling' software may be used to gather more detailed information, which is then potentially traceable.

Officers must not, under any circumstances, use their own personal Social Networking Sites (SNS), profiles or other online accounts to undertake investigative research. The safety of staff is paramount and such practices could potentially put staff or their families at risk of repercussions.

7. COMMUNICATIONS DATA

7.1 Definition

This covers any conduct in relation to a postal service or telecommunications system for obtaining communications data and the disclosure to any person of such data. For these purposes, communications data includes information relating to the use of a postal service or telecommunications system but does not include the contents of the communication itself, content of emails or interaction with websites.

Council Officers do not normally obtain communications data but, given the legislative changes made by IPA 2016, this will be kept under review.

8. AUTHORISATION PROCEDURE

8.1 General

Authorisation is required for the use of directed surveillance, for the conduct and use of sources and for the conduct in relation to a postal service or telecommunication system and the disclosure to any person of such data. Authorisation for directed surveillance can only be granted if the purpose of the surveillance is the prevention or detection of crime(s) punishable by 6 months imprisonment or more, or relates to the sale or alcohol or tobacco to underage persons.

Any officer who undertakes investigations on behalf of the Council shall seek provisional authorisation in writing from an Authorising Officer in relation to any directed surveillance or for the conduct and use of any source. Each provisional authorisation then needs to receive judicial approval before being acted upon.

Flowcharts which may be of use when considering whether to undertake covert surveillance or the use of CHIS are at **Appendices 2 & 3**.

8.2 Who can give Provisional Authorisations?

By law, the 'Authorising Officer' for local authority purposes is any assistant Chief Officer, assistant Head of Service, service manager or equivalent. An Authorising Officer may grant a provisional authorisation, but this authorisation will not take effect until it receives judicial approval (See paragraph 7.4). Please note that certain provisional authorisations, namely those relating to confidential information, vulnerable individuals and juvenile sources, can only be granted by the Chief Executive, or, in her genuine absence, her authorised Deputy.

The Council's authorised posts are listed in **Appendix 1**. This appendix will be kept up to date by the Senior Responsible Officer and added to as needs require. If any council manager wishes to add, delete or substitute a post, a request must be referred to the Senior Responsible Officer for consideration as necessary.

It will be the responsibility of Authorising Officers who have been duly certified to ensure their relevant members of staff are also suitably trained as 'applicants' so as to avoid common mistakes appearing on forms for RIPA authorisations.

Training will be given before Authorising Officers are certified to sign any RIPA forms. A central register of all those individuals who have undergone training will be kept by the RIPA Coordinator.

Authorising Officers will also ensure that staff who report to them follow this guidance document and do not undertake or carry out any form of surveillance without first obtaining the relevant authorisations in compliance with this document.

Authorising Officers must also ensure that, when sending copies of any forms to the RIPA Coordinator, these are sent securely. The increasing use of digitalisation and remote working mean that for most purposes forms will be produced in PDF format and transferred electronically via email or to a shared folder with restricted access. Where hard copy transfer is unavoidable, the forms should be sent in sealed envelopes and marked 'Strictly Private and Confidential'.

Any equipment to be used in any approved surveillance must be properly controlled, recorded and maintained for audit purposes.

8.3 Grounds for Authorisation – the 'necessary & proportionate' test

An Authorising Officer has a number of obligations within the provisions of the Act, which must be met before authorising out any form of surveillance.

An Authorising Officer shall not grant a provisional authorisation for the carrying out of directed surveillance, or for the use of a source unless he believes:

a) that a provisional authorisation is necessary and

b) the provisionally authorised investigation is proportionate to what is sought to be achieved by carrying it out.

For local authority investigations, provisional authorisation is deemed "**necessary**" in the circumstances of the particular case if it is for the purpose of preventing or detecting crime.

Conduct is not deemed "**proportionate**" if the pursuance of the legitimate aim listed above will not justify the interference if the means used to achieve the aim are excessive in the circumstances. Any conduct must meet the objective in question and must not be arbitrary or unfair nor must the impact on any individuals or group be too severe. The conduct must also be the least invasive method of achieving the end and the risk of intrusion into the privacy of persons other than those who are directly the subjects of the investigation must be assessed and taken into account (see Collateral Intrusion below).

Consideration must be given to the seriousness of the offence under consideration. Authorisation for directed surveillance can only be granted if the purpose of the surveillance is the prevention or detection of crime(s) punishable by 6 months imprisonment or more, or relates to the sale or alcohol or tobacco to underage persons. Covert surveillance relating to dog fouling and suspected false addresses will not be deemed a proportionate activity.

Careful consideration needs to be made by authorising officers of all of these points. Such consideration needs to be demonstrated on the authorisation form in the relevant parts. Authorising Officers must exercise their minds every time they are asked to sign a form. They must never sign or rubber stamp the form without thinking about their personal and the Council's responsibilities. Any boxes not needed on the form/s must be clearly marked as being 'not

applicable' or a line put through the same. Great care must also be taken to ensure accurate information is used and inserted in the correct boxes. Reasons for any refusal of an application must also be kept on the form and retained for future audits.

Authorising Officers should not be responsible for authorising investigations or operations in which they are directly involved.

Collateral Intrusion

Before provisionally authorising investigative procedures, the Authorising Officer shall 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). The investigating officer shall take measures, wherever practicable, to avoid or minimise unnecessary intrusion into the lives of those not directly connected with the investigation or operation.

An application for a provisional authorisation shall include an assessment of the risk of any collateral intrusion. The Authorising Officer shall take this into account, when considering the proportionality of the surveillance.

Where an operation unexpectedly interferes with the privacy of individuals who were not the subject of surveillance or covered by the authorisation in some other way, the investigating officer should inform the Authorising Officer who will consider whether it is proportionate to continue.

8.4 Judicial Approval of Provisional Authorisations and Renewals

The Council is only able to grant a provisional authorisation or renewal to conduct covert surveillance. All provisional authorisations and renewals must be approved by the Magistrates Court before surveillance commences.

The Council must apply to the local Magistrates Court for an Order approving the grant or renewal of an authorisation. A template application form and draft Order are included at **Appendix 4** to this policy. In order to obtain judicial approval, the first page of the template form must be completed and submitted along with a copy of the provisional authorisation and any other relevant supporting documents.

The Council does not need to give notice of the application to the person(s) subject to the application or their legal representatives. If the Magistrates Court refuse to approve the application, they may also make an order quashing the provisional authorisation.

The Magistrates will consider the provisionally authorised application or renewal, and will need to satisfy themselves satisfied that:

a) At the time of provisional authorisation, there were reasonable grounds for believing that the tests of necessity and proportionality were satisfied in relation to the authorisation, and that those grounds still exist;

b) That the person who granted provisional authorisation was an appropriately designated person;

c) The provisional grant or renewal of any authorisation or notice was not in breach of any restrictions imposed under RIPA; and

d) Any other conditions provided for by an order made by the Secretary of State were satisfied.

The relevant officers, supported by Legal, will generally make applications for judicial approval to the Magistrates Court on behalf of the Council.

8.5 Urgency

Urgent authorisations are no longer available in relation to directed surveillance or covert human intelligence sources.

8.6 Standard Forms

All authorisations must be in writing.

Standard forms for seeking provisional directed surveillance and covert human intelligence source authorisations are provided at **Appendix 4**. The standard form for obtaining judicial approval is provided at **Appendix 4**. All authorisations shall be sought using the standard forms as amended from time to time.

9. ACTIVITIES BY OTHER PUBLIC AUTHORITIES CONTRACTORS AND PARTNERS

9.1 The investigating officer shall make enquiries of other public authorities e.g. the police whether they are carrying out similar activities if he considers that there is such a possibility in order to ensure that there is no conflict between the activities of this Council and those other public authorities.

9.2 Contractors and Partners

Employees of a private company, such as Capita, are not permitted to make applications to carry out covert surveillance. Any employee of such a company considering the need to carry out surveillance should contact a member of the Council's Legal Team who may make an application on their behalf, ensuring that the Legal Officer is fully briefed on the details of the case and the planned surveillance.

Any employee of a partner organisation considering the need to carry out surveillance should contact a member of the Council's Legal Team who may make an application on their behalf, ensuring that the Legal Officer is fully briefed on the details of the case and the planned surveillance.

10. JOINT INVESTIGATIONS

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

When some other agency (eg police, Customs & Excise, Inland Revenue etc):

(a) wish to use the Council's resources (eg CCTV surveillance systems), that agency must use its own RIPA procedures and, before any officer agrees to allow the Council's resources to be used for the other agency's purposes, he must obtain a copy of that agency's RIPA form for the record and/or relevant extracts from the same which are sufficient for the purposes of protecting the Council and the use of its resources

(b) wish to use the Council's premises for their own RIPA action, the officer should, normally, co-operate with the same, unless there are security or other good operational or managerial reasons as to why the Council's premises should not be used for the agency's activities. In such cases, the Council's own RIPA forms should not be used as the Council is only assisting and not being involved in the RIPA activity of the external agency.

In terms of (a), if the police or other agency wish to use the Council's resources for general surveillance, as opposed to specific RIPA authorisations, an appropriate letter requesting the proposed use, remit, duration, details of who will be undertaking the general surveillance and the purpose of it must be obtained from the police or other agency before any Council resources are made available for the proposed use.

11. DURATION, RENEWALS AND CANCELLATION OF AUTHORISATIONS

11.1 Duration

Authorisations must be reviewed in the time stated and cancelled once no longer needed.

Authorisations last for:

a) 12 months from the date of the judicial approval for the conduct or use of a source (other than a juvenile CHIS which lasts for 4 months only)

b) three months from the date of judicial approval for directed surveillance

However, whether the surveillance is carried out/conducted or not in the relevant period, does not mean that the authorisation is spent. Authorisations do not expire, they have to be reviewed, or cancelled if no longer required.

Communications data

The Office for Communications Data Authorisations (OCDA) commenced its operations in March 2019. OCDA assesses Communications Data applications from public authorities and will make decisions about those applications that strike a fine balance between protection of privacy and risk to public safety. The rules around accessing Communications Data are tightly controlled. Under the Investigatory Powers Act, OCDA will be responsible for ensuring that any applications made by relevant authorities in the UK are assessed independently, rigorously and in line with newly strengthened legislation. OCDA acts as a hub of authorisation expertise, independently assessing applications, holding authorities accountable to robust safeguarding standards, and challenging where required. Local authorities must submit all their communication data applications, via, NAFN for the consideration of OCDA. All applications must be authorised by OCDA prior to any communications data being acquired on behalf of a Local Authority.

11.2 Reviews

The Authorising Officer shall undertake regular reviews of authorisations to assess the need for the surveillance to continue. The results of a review should be recorded on the central record of authorisations. Where the surveillance provides access to confidential information or involves collateral intrusion the officer should conduct frequent reviews.

Standard review forms for directed surveillance and CHIS are attached at **Appendix 4**.

11.3 Renewals

Authorisations may be renewed more than once, if necessary, and the renewal should be kept/recorded as part of the central record of authorisations.

Authorisations can be renewed in writing shortly before the maximum period has expired. An authorisation cannot be renewed after it has expired. The Authorising Officer must consider the matter afresh, including taking into account the benefits of the surveillance to date and any collateral intrusion that has occurred. The renewal will begin on the day when the authorisation would have expired, provided the necessary judicial approval has been obtained.

A further requirement in relation to renewal of covert human intelligence sources, is that judicial approval will only be granted if the Magistrates are satisfied that a review has been carried out, which considers:

- the use made of the source in the period since authorisation was granted (or the last renewal); and
- the tasks given to the source during that period, and the information obtained

from the conduct or use of the source.

and for the purposes of making an Order, the Magistrates have considered the results of that review.

The Authorising Officer who granted or last renewed the authorisation must cancel it if he is satisfied that the investigative procedure no longer meets the criteria upon which it was authorised.

Standard renewal forms for the authorisation of directed surveillance and CHIS are attached at **Appendix 4**.

11.4 Cancellations

An Authorising Officer shall cancel a notice or authorisation as soon as it is no longer necessary, or the conduct is no longer proportionate to what is sought to be achieved.

Cancellation forms for directed surveillance and CHIS are attached at **Appendix 4.**

12. RECORDS

The Council must keep a detailed record of all authorisations, reviews, renewals, cancellations and rejections in departments and a central register of all such forms will be maintained by the RIPA Coordinator.

12.1 Central record of all Authorisations

The RIPA Coordinator to the Council shall hold a centrally retrievable record of all provisional and judicially approved authorisations. The Authorising Officer must notify and forward a copy of any provisional notice or authorisation granted, renewed or cancelled and any judicial approval received or refused within 1 week of the event to the RIPA Coordinator to ensure that the records are regularly updated.

The record will be made available to the relevant Commissioner or an Inspector from the IPCO (Investigatory Powers Commissioner's Office). These records will be retained for a period of three years from the ending of the authorisation. A record will be kept of the dates on which the authorisation notice is started and cancelled.

The records submitted to the RIPA Coordinator shall contain the following information:

a) the type of authorisation or notice

b) the date the provisional authorisation or notice was given;

c) name and rank/grade of the authorising officer;

d) the date judicial approval was received or refused;

e) the unique reference number (URN) of the investigation or operation;

f) the title of the investigation or operation, including a brief description and names of subjects, if known;

g) if the authorisation or notice is renewed, when it was renewed and who authorised the renewal, including the name and rank/grade of the authorising officer and the date of judicial approval;

h) whether the investigation or operation is likely to result in obtaining confidential information;

i) the date the authorisation or notice was cancelled.

The Senior Responsible Officer will monitor the submission of provisional and judicially approved authorisations and notices and give appropriate guidance, from time to time. The SRO must not amend the workings of the Applicant or Authorising Officer to preserve the integrity of different roles.

12.2 **Records maintained in the Department**

The Authorising Officer shall maintain the following documentation ideally in one secure and central location. Maintaining copies in different locations is to be avoided and can complicate the application of retention, review and destruction processes.

a) a copy of the application and provisional authorisation or notice together with a copy of any order of judicial approval or refusal, as well as any supplementary documentation and notification of the approval given by the Authorising Officer;

b) a record of the period over which the surveillance has taken place;

c) the frequency of reviews prescribed by the Authorising Officer;

d) a record of the result of each review of the authorisation or notice;

e) a copy of any renewal of an authorisation or notice, together with judicial approval or refusal and the supporting documentation submitted when the renewal was requested;

f) the date and time when any instruction was given by the Authorising Officer.

g) the unique reference number for the authorisation (URN)

Each form must have a URN provided by the RIPA Coordinator. The Authorising Officers will issue the relevant URN to applicants. The cross-

referencing of each URN takes place within the form for audit purposes. Rejected forms will also have URN's.

12.3 **Other Record of Covert Human Intelligence Sources**

Proper records must be kept of the authorisation and use of a source. An Authorising Officer must not grant a provisional authorisation for the use or conduct of a source unless he believes that there are arrangements in place for ensuring that there is at all times a person with the responsibility for maintaining a record of the use made of the source.

The records shall contain the following information:

(a) the identity of the source;

(b) the identity, where known, used by the source;

(c) any relevant investigating authority other than the Council;

(d) the means by which the source is referred to within each relevant investigating authority;

(e) any other significant information connected with the security and welfare of the source;

(f) any confirmation made by a person granting or renewing an authorisation for the conduct or use of a source that the information in paragraph (d) has been considered and that any identified risks to the security and welfare of the source have where appropriate been properly explained to and understood by the source;

(g) the date when, and the circumstances in which, the source was recruited;

(h) the identities of the persons who, in relation to the source;

i. hold day-to-day responsibility for dealing with the source and for the source's security and welfare

ii. have a general oversight of the use made of the source (not to be the person identified in (h)(i))

iii. have responsibility for maintaining a record of the use made of the source

(i) the periods during which those persons have discharged those responsibilities;

(j) the tasks given to the source and the demands made of him in relation to his activities as a source;

(k) all contacts or communications between the source and a person acting on behalf of any relevant investigating authority;

(l) the information obtained by the conduct or use of the source;

(m) any dissemination of information obtained in that way; and

(n) in the case of a source who is not an undercover operative, every payment, benefit or reward and every offer of a payment, benefit or reward that is made or provided by or on behalf of any relevant investigating authority in respect of the source's activities for the benefit of that or any other relevant investigating authority.

13. SAFEGUARDS FOR RETENTION, REVEW AND DESTRUCTION OF MATERIAL OBTAINED THROUGH COVERT POWERS

Material obtained in the course of criminal investigations and which may be relevant to the investigation must be recorded and retained in accordance with the Criminal Procedure and Investigations Act 1996.

The Council must have in place arrangements for the handling, storage and destruction of material obtained through the use of covert surveillance and compliance with the appropriate data protection requirements must be ensured.

The Council's Information Governance Policy, Strategy and Framework must be adhered to. In addition, before any authorisation is approved, advice on the handling, dissemination, copying, storage, security, retention and destruction of covert surveillance material must be sought from the RIPA Co-ordinating Officer and the ICT Manager, in order to ensure the Council complies with the additional safeguarding obligations contained in the relevant Home Office Codes of Practice.

This Policy document shall be kept under review to ensure it is consistent with the Safeguards chapter of the 2018 Code of Practice, as may be amended. There will be a suitable audit trail for the eventual destruction of product, including the means by which an officer(s) will be designated to check this is being carried out as intended. An additional entry in the Central Record may be used as a suitable means to capture this. The Council's Information Governance Policy and Information Asset Register will on review consider a reference to the Safeguards for RIPA/IPA product with a link to the main Corporate Surveillance Policy section for further advice.

The Council will ensure that internal safeguard policies for retaining, reviewing and disposing of any relevant data are accurate and up-to-date. Authorising Officers will through training have an understanding of any data pathways used for RIPA or IPA data. Authorising Officers will familiarise themselves with retention policies and know who will be personally responsible for retention, review and destruction of data shown on the central record.

All data obtained under IPA and RIPA will be clearly labelled and stored on secure shared corporate repositories (e.g. j drive, kahootz, GIS, Sharepoint as applicable).

All electronic copies of the signed authorisations, will be retained for three years and then disposed of securely, unless it is believed that the records could be relevant to pending or future criminal proceedings, where they must be retained for a suitable further period, commensurate to any subsequent review.

The Council will ensure that all material acquired during covert surveillance is held in secure locations, with clear handling instructions in place when material exchanges hands, and a clear retention, review, destruction (RRD) schedule will be applied to all copies made.

14. CONSEQUENCES OF IGNORING RIPA

RIPA states that if authorisation confers entitlement to engage in a certain conduct and the conduct is in accordance with the authorisation, then **it shall be lawful for all purposes.**

Where there is interference with the right to respect for private and family life guaranteed under Article 8 of the European Convention on Human Rights, and where there is no other source of lawful authority, the consequence of not obtaining an authorisation under RIPA may be that the action is unlawful by virtue of section 6 of the Human Rights Act 1998.

Officers shall seek an authorisation where the directed surveillance, the use of a source or the obtaining or disclosure of communications data is likely to interfere with a person's Article 8 rights to privacy by obtaining private information about that person, whether or not that person is the subject of the investigation or operation. Obtaining an authorisation will ensure that the action is carried out in accordance with law and subject to stringent safeguards against abuse.

15. SCRUTINY OF INVESTIGATORY BODIES

The IPCO (Investigatory Powers Commissioner's Office) has been established under IPA 2016 to facilitate independent scrutiny of the use of RIPA powers by the investigatory bodies that are subject to it. The Commissioners will inspect Councils to ensure compliance with RIPA and can audit/review the Council's policies and procedures, and individual authorisations. Further detail can be found at IPCO – Investigatory Powers Commissioner's Office.

There is also a statutory complaints system welcomed by the Council. The Investigatory Powers Tribunal has been established under RIPA to deal with complaints from members of the public about the use or conduct by public authorities of these powers. The Tribunal is separate from IPCO. The Council welcomes this external scrutiny. It expects its officers to co-operate fully with

these statutory bodies and to bring forward any proposals for improvement that may follow on from an inspection report or a Tribunal hearing.

IF IN DOUBT ADVICE MUST BE SOUGHT FROM THE RIPA COORDINATOR