# REGULATION OF INVESTIGATORY POWERS ACT 2000

# CORPORATE POLICY AND PROCEDURE ON THE USE OF COVERT SURVEILLANCE

| | |
|---|---|
| Title | Regulation of Investigatory Powers Act 2000 |
| Owner | Data Protection Officer |
| Version | 12 |
| Issue date | September 2021 |
| Approved by | Audit and Accounts Committee |
| Next revision due | September 2022 |

# Contents

## INTRODUCTION

1.1 This document sets out the policy and procedures adopted by Basingstoke and Deane Borough Council ("the council") in relation to Part II of the Regulation of Investigatory Powers Act 2000 ("RIPA") and the Investigatory Powers Act 2016. The policy should be read in conjunction with the Home Office Codes of Practice on covert surveillance and covert human intelligence sources; acquisition and disclosure of communications data, and any guidance issued by the Investigatory Powers Commissioner's Office (IPCO)

1.2 For the purpose of this update, references to the Home Office Codes of Practice relate to the latest versions which were issued in September 2018, in relation to covert surveillance and covert human intelligence sources; and May 2015 in relation to the acquisition and disclosure of communications data. References to the OSC Procedures and Guidance document relate to the latest version which was issued in July 2016.

1.3 Recent guidance from the IPCO in respect of data handling and retention safeguards has been reflected in the policy.

1.4 The following terms are used throughout this Policy:

| | |
|---|---|
| RIPA | Regulation of Investigatory Powers Act 2000 |
| CHIS | Covert Human Intelligence Source |
| SPoC | Single Point of Contact |
| SRO | Senior Responsible Officer |
| IPCO | Investigatory Powers Commissioner's Office |
| NAFN | National Anti-Fraud Network |
| CSP | Communications Service Provider |

1.5 It should be noted that any use of activities under RIPA will be as a last resort and council policy is not to undertake such activities unless absolutely necessary.

Further information on RIPA, including guidance on completion of forms and a summary of terms can be found on RIPA - Forms and Guidance (sharepoint.com)

## 2 PURPOSE AND OBJECTIVES

2.1 Directed surveillance, use of a CHIS or acquisition of communications data by or on behalf of the council must be carried out in accordance with this policy. Any such activity must be authorised by one of the Authorising Officers identified in Appendix A. Authorisations for directed surveillance or the use of a CHIS must then be approved by a Magistrate before any covert activity takes place. Staff directly employed by the council and any external agencies working for the council are subject to RIPA whilst they are working in a relevant investigatory capacity.

2.2 The purpose of the policy is to ensure the council is acting lawfully while undertaking its various enforcement functions, ensuring directed surveillance, the use of a Covert Human Intelligence Source (CHIS) or acquisition of communication data is both necessary and proportionate, and takes into account the rights of individuals under Article 8 of the Human Rights Act.

2.3 Surveillance, for the purpose of the Act, includes monitoring, observing or listening to persons, their movements, conversations or other activities and communications. It may be conducted with or without the assistance of a surveillance device and includes the recording of any information obtained.

## 3 ROLES AND RESPOSIBILTIES

3.1 Senior Responsible Officer (SRO):

3.1.1 The role of SRO will be undertaken by the council's Head of Law and Governance

3.1.2 In accordance with good practice the SRO will be responsible for:

- The integrity of the process in place within the council for the management of CHIS and Directed Surveillance;
- Ensuring that all authorising officers are of an appropriate standard;
- Compliance with Part 2 of the Act and with the Home Office Codes of Practice;
- Oversight of the reporting of errors to the relevant Commissioner and the identification of both the cause(s) of errors and the implementation of processes to minimise repetition of errors;
- Engagement with the Investigatory Powers Commissioner's Office (IPCO) inspectors when they conduct their inspections, where applicable; and
- Where necessary, oversight of the implementation of post-inspection action plans approved by the relevant oversight Commissioner.

### 3.2 Authorising Officers

3.2.1 The officers named in Appendix A shall be the only officers within the council who can authorise applications under RIPA in accordance with the procedures set out in section 8 of this policy.

3.3 Each of the Authorising Officers can authorise applications, for onward consideration by a Magistrate. Each Authorising Officer may authorise renewals and cancellations, and undertake reviews, in relation to any investigation carried

out, or proposed to be carried out, by officers. Authorising Officers **may not sub-delegate** their powers in relation to RIPA to other officers.

3.4 The officer who authorises a RIPA application should also carry out the review, renewal and cancellation. If the original Authorising Officer is not available to undertake the review, renewal or cancellation, this can be undertaken by any other Authorising Officer.

3.5 Authorising Officers must have a full understanding of where all relevant data in respect of authorised activities are stored.

3.6 **RIPA Monitoring Officer:**

3.6.1 The post holder named in Appendix A has been appointed RIPA Monitoring Officer.

3.6.2 The RIPA Monitoring Officer shall:-

- have overall responsibility for the management and oversight of requests and authorisations under RIPA;
- issue a unique reference number to each authorisation requested under RIPA (this must be before the application has been authorised);
- retain a copy of the application and authorisation together with any supplementary documentation and notification of the approval given by the authorising officer maintain a central RIPA records file matrix entering the required information as soon as the forms/documents are received in accordance with the relevant Home Office Code of Practice;
- review and monitor all forms and documents received to ensure compliance with the relevant law and guidance and this policy and procedures document and informing the Authorising Officer of any concerns;
- chase failures to submit documents and/or carry out reviews/cancellations;
- be responsible for organising a corporate RIPA training programme;
- ensure corporate awareness of RIPA and its value as a protection to the council is maintained;
- Produce a report to the council's Audit and Accounts Committee on the council's use of RIPA, as detailed in paragraph 3.7.2 below.

3.7 **Councillors**:

3.7.1 Members of the council's Audit and Accounts Committee will approve the RIPA policy on an annual basis.

3.7.2 Members of the council's Audit and Accounts Committee will receive the following information:

| Information to be provided | Frequency |
|---|---|
| The number of RIPA authorisations requested and granted | Annual report, but details of each individual authorisation to be provided to the next available meeting |

| | |
|---|---|
| The number of joint operations where RIPA authorisation has been sought and granted by another authority | Annual report, but details of each individual authorisation to be provided to the next available meeting |
| The number of times social networking sites have been viewed in an investigatory capacity | Report to each meeting of the Committee. Report to be presented by the Chair |

All viewings of social networking sites in an investigatory capacity should be recorded on Social Networking Sites and Investigations (sharepoint.com)

## 4 LOCAL AUTHORITY USE OF RIPA

4.1 RIPA sets out a regulatory framework for the use of covert investigatory techniques by public authorities. RIPA does not provide any powers to carry out covert activities. If such activities are conducted by council officers, then RIPA regulates them in a manner that is compatible with the European Convention on Human Rights (ECHR), particularly Article 8, the right to respect for private and family life.

4.2 RIPA limits local authorities to using three covert techniques, as set out below:

**Directed surveillance** is essentially covert surveillance in places other than residential premises or private vehicles

A **Covert human intelligence source (CHIS)** includes undercover officers, public informants and people who make test purchases (for enforcement purposes)

Acquisition of **Communications data** is the ‘who', ‘when' and ‘where' of a communication, but not the ‘what' (i.e. the content of what was said or written). RIPA groups communications data into three types:

- ‘Traffic data' (which includes information about where the communications are made or received)
- ‘service use information' (such as the type of communication, time sent and its duration); and
- ‘subscriber information' (which includes billing information such as the name, address and bank details of the subscriber of telephone or internet services)

4.3 Under RIPA a local authority can only authorise the acquisition of the less intrusive types of communications data: service use and subscriber information. Under **no circumstances** can local authorities be authorised to obtain traffic data under RIPA.

4.4 Local authorities are **not** permitted to intercept the content of any person's communications and it is an offence to do so without lawful authority.

4.5 Directed surveillance may only be authorised under RIPA 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.

4.6 Local authorities cannot authorise directed surveillance for the purpose of preventing disorder unless this involves a criminal offence(s) punishable (whether on summary conviction or indictment) by a maximum term of at least 6 months' imprisonment. Requests for authorisation must still demonstrate how the activity is both proportionate and necessary.

4.7 A local authority **may not** authorise the use of directed surveillance under RIPA to investigate disorder that does not involve criminal offences or to investigate low-level offences which may include, for example, littering, dog control and flyposting.

4.8 Examples of cases where the offence being investigated attracts a maximum custodial sentence of six months or more include more serious criminal damage and dangerous waste dumping

4.9 Directed surveillance will always be a last resort in an investigation, and use of a CHIS by the council is unlikely. These activities will only be undertaken where there is no other reasonable and less intrusive means of obtaining the information.

4.10 In cases of joint working with other agencies, for example the Department for Work and Pensions or the Police, only one authorisation from one organisation is required. This should be made by the lead authority for the particular investigation. Council officers should satisfy themselves that authorisation has been obtained and be clear exactly what activity has been authorised. All cases of covert surveillance undertaken in joint working with other authorities or organisations will be reported to the Audit and Accounts Committee in accordance with paragraph 3.7.2 above

4.11 For access to communication data, a Single Point of Contact (SPoC) is required to undertake the practical facilitation with the communications service provider (CSP) in order to obtain the data requested. The SPoC must have received training specifically to facilitate lawful acquisition of communications data and effective co-operation between the local authority and CSP.

4.12 The National Anti-Fraud Network (NAFN) provides a SPoC service to local authorities. The council's contact with NAFN is through the Senior Investigator in the Internal Audit Team.

4.13 Compliance with the provisions of RIPA, the Home Office Codes of Practice and this policy and procedures should protect the council, its officers and agencies working on its behalf against legal challenge. Section 27 of RIPA states that “conduct...shall be lawful for all purposes if an authorisation...confers an entitlement to engage in that conduct on the person whose conduct it is and his conduct is in accordance with the authorisation”. If correct procedures are not followed, the council could be rendered liable to claims and the use of the information obtained may be disallowed in any subsequent legal proceedings.

## 5 THE SCOPE OF RIPA AND TYPES OF SURVEILLANCE

5.1 Officers should be aware of the scope and extent of activities covered by the provisions of RIPA. In many cases investigations carried out by council officers will not be subject to RIPA, as they involve overt rather than covert surveillance (see below). An explanation of terms used is set out below:

5.2 **'Surveillance'** includes

- monitoring, observing, listening to persons, watching or following their movements, listening to their conversations and other such activities or communications;
- recording anything mentioned above in the course of authorised surveillance;
- surveillance by, or with the assistance of, appropriate surveillance device(s).

**Surveillance can be overt or covert.**

5.2.1 Covert Surveillance

- Covert Surveillance is surveillance carried out in a manner calculated to ensure that the person subject to the surveillance is unaware that it is, or may be taking place.
- RIPA requires the authorisation of two types of covert surveillance (**directed surveillance** and **intrusive surveillance**) plus the use of covert human intelligence sources (CHIS) or acquisition of communications data.

5.2.2 Directed Surveillance - Chapter 3 of the Home Office guidance – Covert Surveillance and Property Interference - Revised Code of Practice explains that Directed Surveillance is surveillance which:-

- is covert; and
- is not intrusive surveillance (see definition below - the council is prohibited by law from carrying out any intrusive surveillance);
- is not carried out as an immediate response to events where it would not be practicable to obtain authorisation under the Act;
- 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).

5.3 **Private information** in relation to a person includes any information relating to his private and family life, his home and his correspondence. The fact that covert surveillance occurs in a public place or on business premises does not mean that it cannot result in the obtaining of private information about a person. The way a person runs their business may also reveal information about his private life and the private lives of others. Prolonged surveillance targeted on a single person will

undoubtedly result in the obtaining of private information about him/her and others that s/he comes into contact or associates with.

5.4 Private life considerations are particularly likely to arise if several records are to be analysed together in order to establish, for example, a pattern of behaviour, or if one or more pieces of information (whether or not available in the public domain) are covertly (or in some cases overtly) obtained for the purpose of making a permanent record about a person or for subsequent data processing to generate further information. In such circumstances, the totality of information gathered may constitute private information even if individual records do not. Where such conduct includes covert surveillance, a directed surveillance authorisation may be considered appropriate

5.5 Private information may include personal data, such as names, telephone numbers and address details. Where such information is acquired by means of covert surveillance of a person having a reasonable expectation of privacy, a direct surveillance authorisation is appropriate.

5.6 **Overt Surveillance**

5.6.1 Overt Surveillance will include most of the surveillance carried out by the council - there will be nothing secretive, clandestine or hidden about it. For example, signposted CCTV cameras normally amount to overt surveillance (but see 5.6.6 below). In many cases, officers will be going about council business openly (e.g. a parking attendant patrolling a council car park).

5.6.2 However, care must be taken to ensure that officers are not intentionally acting as members of the public in order to disguise their true intent as this may then be considered as covert and require RIPA authorisation.

5.6.3 Similarly, surveillance will be overt if the subject has been told it will happen. This will be the case where a noisemaker is warned that recordings will be made 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 without identifying themselves to the owner/proprietor to check that the conditions are being met. Such warnings should be given to the person concerned in writing.

5.6.4 Overt surveillance does not require any authorisation under RIPA. Neither does **low-level surveillance** consisting of general observations in the course of law enforcement (for example, an officer visiting a site to check whether a criminal offence had been committed). Repeated visits may amount to systematic surveillance however, and require authorisation: if in doubt, advice should be sought from the RIPA Monitoring Officer or the Senior Responsible Officer

5.6.5 Home Office guidance also suggests that the use of equipment such as binoculars or cameras, to reinforce normal sensory perception by enforcement officers as part of *general* observation does not need to be regulated by RIPA, as long as the *systematic* surveillance of an individual is not involved. However, if binoculars or cameras are used in relation to anything taking place on any residential premises or in any private vehicle the surveillance can be intrusive even if the use is only fleeting. Any such surveillance will be intrusive “if it consistently provides information of the same quality as might be expected to be obtained from a device actually present on the premises or in the vehicle”. The quality of the image

obtained rather than the duration of the observation is what is determinative. It should be remembered that the council is **not** permitted to undertake intrusive surveillance.

5.6.6 Similarly, although signposted CCTV cameras do not normally require authorisation, this will be required if the camera(s) are to be directed for a specific purpose which involves prolonged surveillance on a particular person. (See Section 13 for guidance on the authorisation of directed surveillance undertaken by means of the council's CCTV cameras.)

5.6.7 Use of body worn cameras should be overt. Badges should be worn by officers stating body cameras are in use and it should be announced that recording is taking place. In addition, cameras should only be switched on when recording is necessary - for example, when issuing parking tickets.

5.6.8 Surveillance that is unforeseen and undertaken as **an immediate response** to events or circumstances such that it is not reasonably practicable to seek authorisation normally falls outside the definition of directed surveillance and therefore authorisation is not required. However, if a **specific investigation** or **operation is subsequently to follow,** authorisation must be obtained in the usual way before it can commence. In no circumstances will any covert surveillance operation be given backdated authorisation after it has commenced.

## 5.7 Social Networking Sites (SNS)

5.7.1 The Home Office Revised Code of Practice on Covert Surveillance and Property Interference, published in 2018, provides the following guidance in relation to online covert activity:

*'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 following guidance is intended to assist public authorities 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, as set out elsewhere in this code. Where a person acting on behalf of a public authority is intending to engage with others online without disclosing his or her identity, a CHIS authorisation may be needed (paragraphs 4.10 to 4.16 of the Covert Human Intelligence Sources code of practice provide detail on where a CHIS authorisation may be available for online activity).*

*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 a public authority 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 available.*

*As set out below, 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.'*

5.7.2 It is recognised that the use of SNS, can provide useful information for council staff carrying out investigations. These investigations may relate to the various enforcement functions within the council, for example fraud, planning enforcement, licensing or environmental health/crime.

5.7.3 SNS can take many forms. This makes defining SNS difficult, however there are some facets which will be common to all forms of SNS. They will always be a web-based service that allows individuals and/or businesses to construct a public or semi-public profile. Beyond this, SNS can be very diverse, but will often have some, or all, of the following characteristics:

- The ability to show a list of other users with whom they share a connection; often termed “friends” or “followers”;
- The ability to view and browse their list of connections and those made by others within the system;
- Hosting capabilities allowing users to post audio, photographs and/or video content that is viewable by others; and
- Take the form of community-based web sites, online discussion forums, chatrooms

and other social spaces online.

5.7.4 Current examples of the most popular forms of SNS, and therefore the most likely to be of use when conducting investigations into alleged offences, include: Facebook; Twitter; YouTube; Instagram; LinkedIn; and Google.

5.7.5 The Council may utilise SNS when conducting investigations into alleged offences. Whilst the use of SNS to investigate an alleged offence is not automatically considered covert surveillance, its misuse when conducting investigations can mean that it crosses over into the realms of covert and/or targeted surveillance, even when that misuse is inadvertent. It is therefore crucial that the Home Office guidance and provisions within the RIPA, as they relate to covert and directed surveillance, are always followed when using SNS information in investigations.

5.7.6 It is the aim of this Policy to ensure that investigations involving the use of SNS are done so lawfully and correctly so as not to interfere with an accused's human rights and to protect officers carrying out the investigation, and ensure where RIPA authorisation if required, is obtained in advance of the evidence being gathered.

5.7.7 When it is discovered that an individual under investigation has set their SNS account to private, Council officers should not attempt to circumvent those settings under any circumstances. Such attempts would include, but are not limited to:

- sending "friend" or "follow" requests to an individual for the purpose of gathering information;
- setting up or using bogus Social Media profiles to gain access to the individual's private profile,
- contacting the individual through any form of instant messaging or chat function requesting access or information,
- asking family, friends, colleagues or any other third party to gain access on their behalf, or otherwise using the SNS accounts of such people to gain access; or
- any other method which relies on the use of subterfuge or deception.

Officers should not use their own private account to view the SNS account of another individual.

5.7.8 A distinction is made between one-off and repeated visits to an individual's SNS profile. Under Part II of RIPA, authorisation must be sought in order to carry out directed surveillance against an individual. Whilst one-off visits, are unlikely to be considered "directed surveillance" for the purposes of RIPA, repeated or frequent visits may cross over into becoming "directed surveillance" requiring RIPA authorisation. A person's SNS profile should not, for example, be routinely monitored on a daily or weekly basis in search

of updates, as this will require RIPA authorisation. Similarly, if an officer intends to engage with others online without disclosing their identity a CHIS (Covert Human Intelligence Source) authorisation may be needed. For further guidance on these points, officers should contact the Council's SRO.

5.7.9 Regardless of whether the Social Media profile belonging to a suspected offender is set to public or private, it should only ever be used for the purposes of evidence gathering. Interaction or conversation of any kind should be avoided at all costs, and at no stage should a Council officer seek to make contact with the individual through the medium of social media. Any contact that is made may lead to accusations of harassment or, where a level of deception is employed by the officer, entrapment, either of which would be detrimental, or potentially fatal, to any future prosecution that may be considered.

5.8 **Intrusive Surveillance**

5.8.1 Intrusive Surveillance occurs when surveillance:

- is covert;
- relates to residential premises and/or private vehicles; and
- involves the presence of a person in the premises or in the vehicle or is carried out by a surveillance device in the premises/vehicle. Surveillance equipment mounted outside the premises will not be intrusive, unless the device consistently provides information of the same quality and detail as might be expected if they were in the premises/vehicle.

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

## 6 COVERT HUMAN INTELLIGENCE SOURCE

6.1 The use of a covert human intelligence source (CHIS), and his or her conduct, also requires authorisation under RIPA. It is considered unlikely that there will be any circumstances which would require the council to either use a CHIS or operate under cover and advice should be sought from the RIPA Monitoring Officer or the Senior Responsible Officer before any authorisation is applied for or granted.

6.2 A CHIS is defined as someone who establishes or maintains a personal or other relationship for the purpose of

- covertly using the relationship to obtain information or provide access to any information to another person;
- covertly disclosing information obtained by means of that relationship where the relationship is conducted in a manner that is calculated to ensure that one of the parties to the relationship is unaware of its purpose.

These provisions would cover the use of professional witnesses to obtain evidence or information, or officers operating "undercover". Great caution should be exercised in these circumstances.

6.3 The provisions of RIPA relating to CHIS do not apply where a situation would not normally require a relationship to be established for the covert purpose of obtaining information. For example:

- where members of the public volunteer information to the council as part of their normal civic duties;
- where the public contact telephone numbers set up by the council to receive information;
- where members of the public are asked to keep diaries of incidents in relation to, for example, planning enforcement, anti-social behaviour or noise nuisance. However, in certain circumstances, RIPA authorisation may be required if the criteria in section 26(2) of the Act are met.

6.4 If a CHIS is used, both the use of the CHIS and his or her conduct require prior authorisation.

6.5 Special safeguards also apply to the use or conduct of juveniles as a CHIS, that is, those under 18 years old. Paragraph 4.2 of the Home Office guidance 2018 on Covert Human Intelligent Source provides that:

*'On no occasion should the use or conduct of a CHIS under 16 years of age be authorised to give information against their parents or any person who has parental responsibility for them. In other cases, authorisations should not be granted unless the special provisions, contained within the Regulation of Investigatory Powers (Juveniles) Order 2000 (as amended), are satisfied.' (link to the 2000 Order https://www.legislation.gov.uk/uksi/2000/2793/contents/made)*

6.6 Authorisations for juvenile sources must be granted by the Head of Paid Service.

6.7 For the purpose of these rules, the age test is applied at the time of the grant or renewal of the authorisation.

6.8 The Home Office Code of Practice on Covert Human Intelligence Sources contains the following requirements in relation to use of CHIS:

- Public authorities should ensure that arrangements are in place for the proper oversight and management of CHIS, including appointing individual officers as defined in the Act for each CHIS. This is known as a 'handler' and the officer will have day to day responsibility for:
    - Dealing with the CHIS on behalf of the authority concerned;
    - directing the day to day activities of the CHIS;
    - recording the information supplied by the CHIS; and
    - monitoring the CHIS's security and welfare
- the handler of a CHIS will usually be of a rank or position below that of the authorising officer
- In addition to a handler, a 'controller' will also be appointed. This officer will be responsible for the management and supervision of the handler and general oversight of the use of the CHIS.

6.9 **Note 251 of the OSC's 2016 Procedures & Guidance document states:**

*251. A local authority may prefer to seek the assistance of the police or another public authority to manage its CHIS. In such a case a written protocol between the parties should be produced in order to ensure that an identified CHIS is properly managed (see CHIS Code of Practice 6.12). In the absence of such an agreement the local authority must be capable of fulfilling its statutory responsibilities.*

## 7 COMMUNICATIONS DATA

7.1 Section 73 of the Investigatory Powers Act 2016 provides that the Council, as a local authority, is a relevant public authority for the purposes of Part 3 of this Act (Authorisations for Obtaining Communications Data).

7.2 Subsection (3) provides that local authorities may only acquire communications data for the purpose of preventing or detecting crime or of preventing disorder.

7.3 Local authorities are only able to obtain communications data if they are party to a collaboration agreement as certified by the Secretary of State. The Council currently uses the National Anti-Fraud Network (NAFN) as a shared Single Point of Contact (SPoC) service.

7.4 Council authorisations to obtain communications data can only take effect if approved by the Office of Communications Data Authorisations (OCDA) once all the internal authorisation processes have been completed, including consultation with a NAFN Single Point of Contact (SPoC), but before the SPoC requests the data from the Telecommunications Provider (TO).

## 8 AUTHORISATION PROCEDURES

8.1 **Any directed surveillance, or the use of a CHIS undertaken by or on behalf of the council must be carried out in accordance with RIPA and must not commence until authorisation has been granted and has been approved by a relevant judicial authority**. If such activities are undertaken without authorisation the RIPA Monitoring Officer or Senior Responsible Officer must be advised immediately. Only those officers employed in the designated "Authorising Officer Posts" set out in Appendix A can authorise an application under RIPA. Once authorised, the application must be presented to a Magistrate for final approval.

8.2 Officers must discuss the need to undertake directed surveillance with their line manager before seeking an authorisation. **All other reasonable and less intrusive options to gain the required information must be considered before an authorisation is applied for and the RIPA application must detail why these options have failed or have been considered not appropriate in the circumstances of the individual investigation.**

8.3 All applications for authorisation must be made on the appropriate form. Guidance on completing the forms can be found on the council's intranet, RIPA - Forms and Guidance (sharepoint.com) together with a procedure for obtaining judicial approval. In the event of any query, officers making, or authorising applications should consult the RIPA Monitoring Officer or the Senior Responsible Officer. The RIPA Monitoring Officer should be contacted prior to the completion of a RIPA application form so that a Unique Reference Number can be allocated.

8.4 Authorisations will not take effect until the relevant judicial authority has made an order approving the grant of the authorisation. The relevant judicial authority in England and Wales is a Magistrate. **It is vital that any surveillance for which authorisation has been sought does not start until such time as it has been approved by a Magistrate**

8.5 It is necessary for the council to obtain judicial approval for all initial RIPA authorisations/applications and renewals. **There is no requirement for the Magistrate to consider either cancellations or internal reviews.**

8.6 The procedure for obtaining Magistrate approval can be found on RIPA Guidance - Crime Threshold and Magistrate Approval.docx (sharepoint.com)

8.7 In the unlikely event that officers find it necessary to seek authorisation for the use of a CHIS, additional safeguards must be considered and advice must first be sought from the RIPA Monitoring Officer or Senior Responsible Officer.

8.8 In any case where it is likely that **confidential information** may be acquired by directed surveillance or by the use or conduct of a source, **the Authorised Officer who may grant authorisation is the Head of Paid Service or, in his absence, the person acting as Head of Paid Service.**

8.9 **Confidential information** consists of communications subject to *legal privilege*, communications between a Member of Parliament and another person on constituency matters, confidential personal information, or confidential journalistic material. So, for example, extra care should be taken where, through the use of surveillance, it is likely that knowledge will be acquired of communications between a minister of religion and an individual relating to the latter's spiritual welfare, or between a Member of Parliament and a constituent relating to constituency matters, or wherever matters of medical or journalistic confidentiality may be involved

8.10 Covert surveillance of all legal consultations should be considered intrusive.

8.11 When considering an application, Authorising Officers must:

(a) have regard to the contents of this document, the training provided, and any other guidance or advice given by the RIPA Monitoring Officer or the Senior Responsible Officer;

(b) satisfy his/herself that the RIPA authorisation will be:

(i) **in accordance with the law**;
(ii) **necessary** in the circumstances of the particular case; and
(iii) **proportionate** to what it seeks to achieve.

(c) assess whether or not the proposed surveillance is proportionate, considering the following elements:

- The custodial sentence applicable to the offence being investigated;
- Balancing the size and scope of the proposed activity against the gravity and extent of the perceived crime or offence;
- Explaining how and why the methods to be adopted will cause the least possible intrusion on the subject and others;
- Whether the activity is an appropriate use of the legislation and a reasonable way, having considered all practical alternatives, of obtaining the necessary result;
- Evidencing, as far as reasonably practicable, what other methods had been considered and why they were not implemented.

(d) take into account the risk of intrusion into the privacy of persons other than the specified subject of the surveillance (called ‘collateral intrusion'), and consider whether any measures should be taken to avoid or minimise collateral intrusion as far as possible (the degree of likely collateral intrusion will also be relevant to assessing whether the proposed surveillance is proportionate);

(e) consider any issues which may arise in relation to the health and safety of council employees and agents, and ensure that a risk assessment has been undertaken if appropriate.

8.12 When authorising the conduct or use of a CHIS, the Authorising Officer must also:

(a) be satisfied that the conduct and/or use of the CHIS is proportionate to the objective sought to be achieved;
(b) be satisfied that appropriate arrangements are in place for the management and oversight of the CHIS. These arrangements must address health and safety issues by the carrying out of a formal and recorded risk assessment;
(c) consider the likely degree of intrusion for all those potentially affected;
(d) consider any adverse impact on community confidence that may result from the use or conduct of the CHIS or the information obtained; and
(e) ensure that records contain the required particulars of the CHIS and that these are not available except on a 'need to know' basis.

8.13 Authorising Officers should consult the RIPA Monitoring Officer or the Senior Responsible Officer before authorising the use of conduct of a CHIS to ensure that all legal requirements are complied with.

8.14 If an application is granted, the Authorising Officer must set a date for its review, and ensure that it is reviewed on that date (see 10.2 below). Records must be kept in relation to all RIPA applications and authorisations in accordance with paragraph 14 below, and to facilitate this, each investigation or operation should be given a unique reference number (URN) on the application form by the RIPA Monitoring Officer. This should be in the form:

Year /Business Unit/ Number of Application.

Any subsequent forms (e.g. renewals or cancellations) relating to the same investigation or operation should be identified by means of the same URN.

## 9 URGENT AUTHORISATIONS

9.1 It is no longer possible for urgent authorisations to be given orally. However, a Magistrate may consider an authorisation out of hours in **exceptional** circumstances.

## 10 DURATION OF AUTHORISATIONS

10.1 Authorisations will have effect until the date for expiry specified on the relevant form. They must be granted for the designated period of three months for directed surveillance, 12 months for the use or conduct of a CHIS, or where the CHIS is a juvenile, 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, and one month for the acquisition of communications data. **No further operations should be carried out after the expiry of the relevant authorisation unless it has been renewed.** It will be the responsibility of the officer in charge of an investigation to ensure that any directed surveillance or use of a CHIS is only undertaken under an appropriate and valid authorisation, and therefore, he/she should be mindful of the date when authorisations and renewals will cease to have effect. The RIPA Monitoring Officer will perform an auditing role in this respect **but the primary responsibility rests with the officer in charge of the investigation.**

10.2 Authorisations should be reviewed at appropriate intervals in order to update the Authorising Officer on progress on the investigation and whether the authorisation is no longer required. Review periods should be set by the Authorising Officer, but should normally take place on a monthly basis unless the Authorising Officer considers that they should take place more or less frequently (if so, the reasons should be recorded). If the surveillance provides access to confidential information or involves collateral intrusion, there will be a need to review the authorisation frequently. The results of reviews should be recorded on the appropriate form.

10.3 All authorisations **must** be cancelled as soon as they are no longer necessary. Even if an authorisation has reached its time limit and has ceased to have effect, it does not lapse and must still be formally cancelled. The responsibility for ensuring that authorisations are cancelled rests primarily with the officer in charge of the investigation, who should submit a request for cancellation on the appropriate form. However, if the Authorising Officer who authorised any directed surveillance or the use or conduct of a CHIS (or any Authorising Officer who has taken over their duties) is satisfied that it no longer meets the criteria upon which it was authorised, s/he must cancel it and record that fact in writing even in the absence of any request for cancellation.

10.4 If it is required, a renewal must be authorised prior to the expiry of the original authorisation. Applications for renewal should be made on the appropriate form shortly before the original authorisation period is due to expire. Officers must take account of factors which may delay the renewal process (e.g. intervening weekends or the availability of the relevant authorising officer and a Magistrate to consider the application). 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. Renewals of an authorisation may be granted more than once, provided the criteria for granting that authorisation are still met. However, if the reason for requiring the authorisation has changed from the purpose for which it was originally granted, then it should be cancelled, and new authorisation sought. The renewal will begin on the day when the original authorisation would otherwise have expired.

## 11 MATERIAL OBTAINED DURING INVESTIGATIONS

11.1 Generally, all material (in whatever media) obtained or produced during the course of investigations subject to RIPA authorisations should be processed, stored and destroyed in accordance with the requirements of the General Data Protection Regulation, Data Protection Act 2018, the Freedom of Information Act 2000, any other legal requirements, including those of confidentiality, and the council's policies and procedures currently in force relating to document retention. The following paragraphs give guidance on some specific situations, but advice should be sought from the RIPA Monitoring Officer or the Senior Responsible Officer where appropriate.

11.2 Where material is obtained during the course of an investigation which might be relevant to that investigation, or another investigation, or to pending or future civil or criminal proceedings, then it should **not** be destroyed, but retained in accordance with legal disclosure requirements. All such material should be clearly labelled and stored in such a way to enable compliance with data retention and disposal.

11.3 Where material is obtained, which is not related to a criminal or other investigation or to any person who is the subject of the investigation, and there is no reason to suspect that it will be relevant to any future civil or criminal proceedings, it should be destroyed immediately.

11.4 Material obtained in the course of an investigation may be used in connection with investigations other than the one that the relevant authorisation was issued for. However, the use or disclosure of such material outside the council, unless directed by any court order, should only be considered in exceptional circumstances, and in accordance with advice from the RIPA Monitoring Officer or the Senior Responsible Officer.

11.5 Where material obtained is of a confidential nature then the following additional precautions should be taken:

- Confidential material should not be retained or copied unless it is necessary for a specified purpose;
- Confidential material should only be disseminated in accordance with legal advice that it is necessary to do so for a specific purpose;
- Confidential material which is retained should be marked with a warning of its confidential nature. Safeguards should be put in place to ensure that such material does not come into the possession of any person where to do so might prejudice the outcome of any civil or criminal proceedings;
- Confidential material should be destroyed as soon possible after its use for the specified purpose.

If there is any doubt as to whether material is of a confidential nature, advice should be sought from the RIPA Monitoring Officer or the Senior Responsible Officer.

## 12 ASSESSMENT AND REVIEW

12.1 Following completion of any investigation/operation involving the use of RIPA, an assessment should be undertaken. This should detail the information obtained and how it was used to take the case forward

12.2 The assessment form will be provided by the RIPA Monitoring Officer, should retain the same reference and be kept with the original RIPA paperwork

12.3 The SRO will undertake periodic reviews of the assessment forms and may provide these records as part of any inspection by the Office of Surveillance Commissioners.

12.4 Assessment forms will be reported to the next available meeting of Audit and Accounts Committee

## 13 CCTV AND DIRECTED SURVEILLANCE

13.1 The use of CCTV must be accompanied by clear signage in order for any monitoring to be overt. If it is intended to use CCTV for covert monitoring, for example by using either hidden cameras or without any signs warning that CCTV is in operation, then RIPA authorisation is likely to be required.

13.2 **Note 272 of the OSC's 2016 Procedures & Guidance document:**

*272. It is recommended that a law enforcement agency should obtain a written protocol with a local authority if the latter's CCTV system is to be used for directed surveillance. Any such protocol should be drawn up centrally in order to ensure a unified approach. The protocol should include a requirement that the local authority should see the authorisation (redacted if necessary to prevent the disclosure of sensitive information) and only allow its equipment to be used in accordance with it.*

## 14 RECORDS MANAGEMENT

14.1 Records shall be maintained for a period of at least **three years** from the cancellation of the authorisation. Following which they shall be securely destroyed in accordance with the council's Retention and Disposal Policy.

14.2 A copy of all completed RIPA forms, including applications (whether granted or refused), authorisations, reviews, renewals and cancellations, must be forwarded by the Authorising Officer to the RIPA Monitoring Officer within **five working days** of the date of the relevant decision. All documents should be sent in sealed envelopes marked “For Your Eyes Only”.

14.3 Applicants and Authorising Officers may keep copies of completed RIPA forms, but care must be taken to ensure any copies are stored securely and disposed of in accordance with the council's retention and disposal policy. It is good practice for officers who will be carrying out surveillance to retain a copy of the authorisation as a reminder of exactly what has been authorised. Under the Criminal Procedure and Investigations Act, case files are required to hold original documents for court action.

14.4 All data obtained under RIPA must be clearly labelled and stored in such a way to enable compliance with data retention and disposal. This requirement will apply to information which is shared with other teams for the purpose of any investigation or to determine legal action to be undertaken.

14.5 All data obtained under RIPA must be stored in a secure manner using password protection or restricted access files.

14.6 All recipients of data obtained under RIPA must ensure that it is retained only as long as is necessary and in accordance with the council's retention schedule. Disposal of data must be recorded on the disposal log which can be found on Information Management - Information Disposal Log - Sinbad View (sharepoint.com)

14.7 Officers within the same team who need to be aware of the investigation, should be directed to where data is held on the relevant computer system (for example Uniform or Iken), rather than multiple copies of the data being emailed to

individuals.

14.8 The following additional information should also be maintained by the Senior Responsible Officer or RIPA Monitoring Officer in relation to any CHIS:

- any risk assessment in relation to the source;
- the circumstances in which tasks were given to the source;
- the value of the source to the investigating authority;

14.9 By law, an Authorising Officer must not grant authority for the use of a CHIS unless s/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 CHIS. Certain particulars must be included in the records relating to each CHIS, and the records must be kept confidential. Further advice should be sought from the RIPA Monitoring Officer or Senior Responsible Officer on this point if authority is proposed to be granted for the use of a CHIS.

14.10 A 'Surveillance Log Book' should be completed by the investigating officer(s) to record all operational details of authorised covert surveillance or the use of a CHIS. Each service will also maintain a record of the issue and movement of all Surveillance Log Books.

14.11 All RIPA records, whether in original form or copies shall be kept in secure locked storage when not in use.

## 15 NON-RIPA

15.1 Due to the changes brought about by the Protection of Freedoms Act 2012, there may be circumstances whereby it is necessary, and proportionate, to carry out covert surveillance for activities which do not meet the crime threshold set out in paragraph 4.5 above

15.2 In such circumstances, staff must complete a non-RIPA form, setting out why such activity is necessary and proportionate and giving due consideration to any potential collateral intrusion

15.3 Non-RIPA forms must be authorised by an OMG level manager. However, if the activity relates to an investigation against a member of staff, authorisation must be provided by the Head of HR and Organisational Development, or one of the council's Executive Directors

15.4 Full guidance on non-RIPA can be found on Non-RIPA (sharepoint.com)

## 16 TRAINING

16.1 Appropriate corporate training will be arranged by the RIPA Monitoring Officer for all officers likely to make applications or authorise them.

16.2 The RIPA Monitoring Officer will ensure suitable training is in place for all new members of staff who undertake an enforcement role. This may be by way of a briefing to officers or an e-learning module. Managers of enforcement teams must ensure new staff undertake RIPA training within six months of their starting date

16.3 Authorising Officers must receive training on an annual basis. This may be by way of a briefing or an e-learning module.

16.4 All other identified staff will be required to attend annual training, either by way of a briefing or an e-learning module. It is the responsibility of managers of enforcement teams in particular, to ensure relevant staff are identified and receive such training.

16.5 Officers may in any event supplement this corporate training by attending appropriate external training courses and seminars. The cost of such external training should be met from the budget of the individual Business Unit.

16.6 No officer will be permitted to undertake the role of Applicant or Authorising Officer unless she/he has undergone suitable training approved by the RIPA Monitoring Officer.

16.7 It is each officer's responsibility to ensure that all training, whether internal or external, is booked and approved via HR Pro in accordance with corporate training policies and procedures.

16.8 This Policy will apply to all council staff and contractors employed by the council. All relevant council contracts will include a term that this Policy is to be observed by any contractor operating on behalf of the council.

## APPENDIX A - ROLES AND RESPONSIBILITIES

### AUTHORISING OFFICERS

| Name | Post Held |
|---|---|
| Russell O'Keefe | Chief Executive |
| Ian Boll | Executive Director of Borough Development and Deputy Chief Executive |
| Rebecca Emmett | Executive Director of Residents Services |
| Sue Cuerden | Executive Director of Corporate Services |

For the purpose of paragraph 8.8, the Chief Executive is the Head of Paid Service and the Executive Director of Borough Development will deputise as required.

### SENIOR RESPONSIBLE OFFICER AND RIPA MONITORING OFFICER

| Name | Post Held |
|---|---|
| Fiona Thomsen Head of Law and Governance | Senior Responsible Officer |
| Jackie Tatam<br>Data Protection Officer | RIPA Monitoring Officer |