Appendix A

The Regulation of Investigatory Powers Act 2000 (RIPA)

CORPORATE POLICY AND PROCEDURES

Version 8 – July 2024

FAREHAM
BOROUGH COUNCIL

Contents

Appendices

1: INTRODUCTION

1.1 Summary

This document is intended to provide officers with guidance on how to carry out certain investigatory procedures in compliance with the law.

RIPA covers the authorisation of directed surveillance, the authorisation of CHIS sources and the authorisation of obtaining communications data. An authorisation under RIPA will provide lawful authority for the investigating officer to carry out these activities.

It should be noted that officers of the councils are only legally permitted to use surveillance and CHIS powers for the purpose of the **prevention or detection of crime(s)** punishable by **6 months** imprisonment or more, or in investigations relating to the sale of alcohol or tobacco to underage persons.

Where the power to be used is the acquisition of "event" communications data then the threshold increases and councils are only legally permitted to use these powers for the purpose of the **prevention or detection of crime(s)** punishable by **12 months** imprisonment or more. However, there is no threshold for the acquisition of "entity" communications data.

It is also stressed that the use of covert powers should be a last resort option when undertaking an investigation and only then if the prevention or detection of crime could not be achieved without the information provided by these activities.

1.2 Corporate Oversight

A **Senior Responsible Officer** will be appointed to ensure the integrity of the process within the Council and its compliance with RIPA. They will have responsibility for:

- the oversight of reporting of errors to the relevant oversight commissioner;
- engaging with relevant inspectors during their inspections and where necessary, oversight of the implementation of any post-inspection action plan.;
- ensure that Members regularly review the Council's use of RIPA.

RIPA and this document are important for the effective and efficient operation of the Council's actions with regard to the investigatory processes covered by this **policy**. This document will, therefore be kept under regular review by the Senior Responsible Officer and the outcomes of this review will be presented to the Executive 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.

The **RIPA Co-ordinator** will carry out a periodic **review of forms** that are open for a long time or need a cancellation form completing, and will identify any links from forms to the Central Register that are missing.

The **Senior Responsible Officer** will carry out a periodic sample check of the quality of RIPA authorisations, renewals and cancellations that feed into the report prepared for the

Audit and Governance Committee. The results of this review will be recorded on the Central Register and will be used to identify any guidance or individual or corporate training needed.

The **Audit and Governance Committee** will consider an annual report on the use of the powers covered by the Act to ensure that it is being used consistently with the local authority's policy and that the policy remains fit for purpose.

1.3 Assistance with Understanding How to Comply

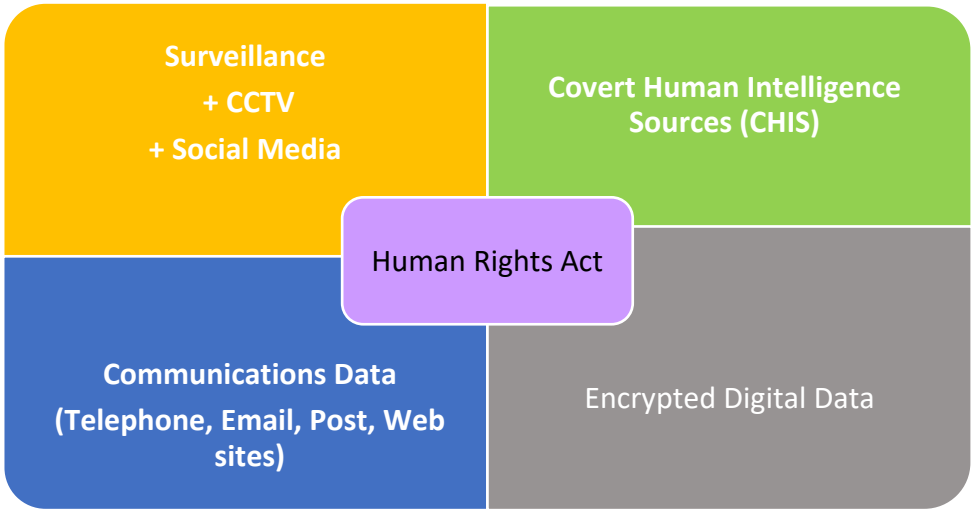
Each officer of the Council with responsibilities for the conduct of investigations, shall, before carrying out any investigation involving RIPA, undertake appropriate training to ensure that investigations and operations that he/she carries out will be conducted lawfully.

Any officer considering the use of RIPA for the first time should first consult the RIPA Co-ordinator (or Senior Responsible Officer) as listed in Appendix B.

2: BACKGROUND

2.1 Relevant Law

The **Regulation of Investigatory Powers Act 2000** ('RIPA') brought into force the regulation of covert investigation by a number of bodies, including local authorities. It covers the following investigatory procedures:



The following acts have supplemented or made further changes to the law:

i) **Lawful Business Practice Regulations 2000**
ii) **The Protection of Freedoms Act 2012** (introduced the need for Judicial approval)
iii) **Data Retention and Investigatory Powers Act 2014** (DRIPA)
iv) **Investigatory Powers Act 2016**

In terms of monitoring of employee 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.

These are covered by the separate Procedure Note for Directed Monitoring of Employees. RIPA forms should only be used where **relevant** and they will only be relevant where the **criteria** listed on the forms are fully met.

2.2 Codes of Practice

Officers must also take into account the Codes of Practice issued by the Home Office with additional policy documents issued by the Investigatory Powers Commissioner's Office.

These can be found on the following websites:

https://www.gov.uk/government/collections/ripa-codes

https://www.ipco.org.uk/

Local copies may be found at: S:\Corporate\Policies & Procedures\RIPA\e. NATIONAL GUIDANCE

The latest Code of Practice for Covert Surveillance also covers interference with property or with wireless telegraphy as governed by Part III of the Police Act 1997. It should be noted that Council officers are **not** permitted to undertake this type of activity.

2.3 The Human Rights Act

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 citizens, their home and 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 citizens' rights 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)

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, and/or the Council could be ordered to pay compensation. **It is essential, therefore, that all involved with RIPA comply with this document and any further corporate guidance that may be issued, from time to time.**

2.4 Consequences of Ignoring the Legislation

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.

3: SURVEILLANCE

3.1 Surveillance Covered by this Policy

Surveillance is covered by this Policy when it is:

- Directed
- Covert
- 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.

3.2 Intrusive Surveillance

Surveillance becomes intrusive if the 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, but 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.

Where surveillance is carried out by a device designed or adapted principally for the purpose of providing information about the location of a vehicle, the activity is directed surveillance.

Commercial premises and vehicles are therefore excluded from intrusive surveillance.

Currently, local authorities are not authorised to carry out INTRUSIVE surveillance.

3.3 Identifying Directed Surveillance

Ask yourself the following questions, or follow the flowchart attached as Appendix C:

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 (e.g. in the case of most test purchases), and/or will be going about Council business openly (e.g. a market inspector walking through markets).

Similarly, surveillance will be **overt** if the subject has been told it will happen (e.g. 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.

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.

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. 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 police officer would not require an authorisation to conceal himself and observe a suspicious person that he came across in the course of a patrol.

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

3.4 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.

Only Authorising Officers designated as a higher level authoriser, in Appendix B, can approve an application which may involve confidential information.

3.5 Use of CCTV and ANPR

Although, the provisions of the Act do not normally cover the use of overt CCTV surveillance systems or Automated Number Plate Recognition (ANPR) in car parks, since members of the public are aware that such systems are in use, there may be occasions when public authorities use overt CCTV systems and/or ANPR 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: COVERT HUMAN INTELLIGENCE SOURCES (CHIS)

4.1 What is a CHIS?

A person is a **source** if:

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

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

(c) they covertly disclose 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 and officers working undercover.

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.

The use or conduct of a source to obtain knowledge of matters subject to **legal privilege** must be subject to the prior approval of the Commissioner.

Carrying out test purchases will not require the purchaser to establish a relationship with the supplier with the covert purpose of obtaining information and, therefore, the purchaser will not normally be a CHIS. For example, authorisation would not normally be required for test purchases carried out in the ordinary course of business (e.g. walking into a shop and purchasing a product over the counter). 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.

However, a member of the public may in reality be a CHIS if they provide information covertly obtained in the course of, or as a result of, a personal or other relationship. If this information is acted on, a duty of care would be owed and the onus on the public authority to manage

human sources properly. The consideration is the manner in which the information has been obtained (i.e. as a result of a relationship established or maintained for a covert purpose), not whether the informant has been tasked to obtain information for the Council.

An authorisation under RIPA will provide lawful authority for the use of a source. Authorising Officers should be alive to the possibility of "status drift". Authorising Officers when deciding whether to grant an authorisation, should take account of the difference between a volunteer of information already known to the individual and the relevance of the exploitation of a relationship for a covert purpose.

4.2 Security and Welfare of the CHIS?

The Authorising Officer shall ensure that arrangements are in place for the proper oversight and management of sources, including appointing the following individual officers for each source:

a) A "**Handler**" who will have day-to-day responsibility for:

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

The Handler will usually be of a rank or position below that of the Authorising Officer.

b) A "**Controller**" who will be responsible for the management and supervision of the "handler" and general oversight of the use of the CHIS.

Officers using a source shall consider the safety and welfare of that source (even after cancellation of the authorisation), and the foreseeable consequences to others of the tasks they are asked to carry out. The Authorising Officer shall carry out a risk assessment before authorising the source.

Only Authorising Officers designated as a higher level authoriser, in Appendix B, can approve an application can authorise the **use of vulnerable individuals and juvenile sources.**

The Authorising Officer shall have regard to the special safeguards and provisions that apply to vulnerable individuals and juvenile sources, more particularly set out in the latest Home Office Covert Human Intelligence Source Code of Practice.

5: SOCIAL MEDIA

5.1 Social Media and Directed Covert Surveillance / CHIS

Investigations using social networking sites on the internet such as Facebook, Netlog, Bebo and Myspace, or other open source sites such as Ebay, may fall into the definition of directed covert surveillance if:

(a) The site is not being accessed by the Councils "corporate" registration but by using an individual account aimed at hiding the identity or presence of the investigator.

(b) The site is being used to regularly monitor and record a person's activities, contents of postings or relationships. and

(c) The monitoring is likely to identify private information about the person and/or third parties.

Even though data may be deemed published and no longer under the control of the author, it is unwise to regard it as 'open source' or publicly available. The author has a reasonable expectation of privacy if access controls are applied. In some cases, data may be deemed private communication still in transmission.

If it is necessary and proportionate for a public authority to breach covertly the access controls then a **directed surveillance** RIPA authorisation must be obtained which assesses the level of intrusion on the subject and the third parties they are interacting with, balanced against the seriousness of the investigation and potential benefit to the investigation of the activity being conducted.

If the nature of the activity involves establishing or maintaining any form of relationship with the subject, their colleagues or friends with a view to obtaining information, then this activity by a Council employee or someone acting on their behalf, requires authorisation to use a **Covert Human Intelligence Source.**

5.2 Activity not permitted

Officers, or someone acting on their behalf, must not:

- Set up a false identity for a covert purpose without authorisation

- Adopt the identity of a person known, or likely to be known, to the subject of interest or users of the site without a) RIPA authorisation, b) the consent of the person whose identity is used, and c) without considering the protection of that person whose identity is being used. The consent must be explicit.

- Use their personal social network login details to view individuals under investigation

5.3 Further Guidance and Examples on whether Authorisation is 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, if reasonable steps have been taken to inform the public or particular individuals that the surveillance is or may be taking place, this can be regarded as overt and a directed surveillance authorisation will not normally be available.

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 the Council interferes with a person's private life includes a consideration of the nature of the Council'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 the Council 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.

Example 1: A simple internet search on a name, address or telephone number to find out whether a subject of interest has an online presence is unlikely to need an authorisation. However, if having found an individual's social media profile or identity it is decided to monitor it or extract information from it for retention in a record because it is relevant to an investigation or operation, authorisation should then be considered.

Example 2: Initial examination of an individual's online profile to establish whether they are of relevance to an investigation is unlikely to need an authorisation. Visiting a website would not normally amount to surveillance, but if during that visit it is intended to extract and record information to establish a profile including information such as identity, pattern of life, habits, intentions or associations, it may be advisable to have in place an authorisation even for that single visit. The purpose of the visit may be relevant as to whether an authorisation should be sought.

Example 3: General monitoring of the internet in circumstances where it is not part of a specific, ongoing investigation or operation does not require RIPA authorisation. This includes any monitoring that is intended to identify themes, trends, possible indicators of criminality or other factors that may influence operational strategies or deployments. It may also include the discovery of previously unknown subjects of interest, but once it is decided to monitor those individuals as part of an ongoing operation or investigation, authorisation should be considered.

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

Example 4 : Researchers within a public authority using automated monitoring tools to search for common terminology used online for illegal purposes will not normally require a directed surveillance authorisation. Similarly, general analysis of data by public authorities either directly or through a third party for predictive purposes (e.g. identifying crime hotspots or analysing trends) is not usually directed surveillance. In such cases, the focus on individuals or groups is likely to be sufficiently cursory that it would not meet the definition of surveillance. But officers should be aware of the possibility that the broad thematic research may evolve, and that authorisation may be appropriate at the point where it begins to focus on specific individuals or groups. If specific names or other identifiers of an individual or group are applied to the search or analysis, an authorisation should be considered.

6: COMMUNICATIONS DATA

6.1 Background and Summary

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).

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

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.

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).

6.2 What is Communications data?

Methods of communication include:

- Email

- Post
- Internet services (web pages)
- Fixed Line Phones
- Mobile Phones

The term 'communications data' includes the 'who', 'when', 'where' and 'how' of a communication but not the content, i.e. what was said or written.

All communications data held by a telecommunication operator or obtainable from a telecommunications system falls into two categories:

- **Entity data (formerly Subscriber Data)** – this data is about entities or links between them and describes or identifies the entity but does not include information about individual events. Entities could be individuals, groups and objects (such as mobile phones or other communications devices).

Examples include phone numbers or other identifiers linked to communications devices; or an IP address allocated to an individual by an internet access provider.

Subscriber data includes the name, address and telephone numbers of those contacted, billing addresses, account information and web addresses visited etc.

- **Events data (formerly Service use and Traffic Data)** – this data identifies or describes events in relation to a telecommunications system which consist of one or more entities engaging in an activity at a specific point, or points, in time. Examples include the fact that someone has sent or received an email, phone call, text or social media message; the location of a person when they made a mobile phone call or the Wi-Fi hotspot that their phone connected to; or the destination IP address that an individual has connected to online.

Communications data in relation to a **postal service** includes:

- Postal data which is or has been comprised in or attached to a communication for the purpose of the service by which it is transmitted;
- Data relating to the use made by a person of a postal service;
- Information held or obtained by a TO about persons to whom the TO provides or has provided a communications service and which relates to the provision of the service

Local authorities cannot INTERCEPT a communication during transmission or before receipt by the designated recipient.

6.3 Serious Crime Threshold

From 1st November 2018, an amendment to RIPA came into force adding a serious crime threshold to the acquisition of Event (service use or traffic data); but not Entity data. This means that where an application is for the crime statutory purpose (S60A(7)(b)) to acquire event data, the crime must be a serious crime.

Local authorities can only request **Event** communication data to assist an investigation into a crime which meets one or more of the following definitions:

- **12 months (or more) imprisonment** - an offence that is capable of attracting a prison sentence of 12 months or more
- **Corporate Body** - an offence by a person who is not an individual
- **S81 Offence** - an offence falling within the definition of serious crime in S81(3)(b) of the IPA where the conduct involves the use of violence, results in substantial financial gain or is by a large number of persons in pursuit of a common purpose;
- **Communication Offence** - an offence which involves, as an integral part of it, the sending of a communication
- **Breach of Privacy** - an offence which involves, as an integral part of it, a breach of a person's privacy

7: AUTHORISATION PROCEDURE

7.1 General Authorisation

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, hereto referred to as the "Investigatory powers".

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

The authorising officer should also ensure that they clearly set out what activity and equipment has been authorised in order that those using the powers are clear on what has been sanctioned (as per the R v Sutherland ruling).

The Council`s list of current officers who have been assigned and trained to act as Authorising Officers (or Approved Ranks for communications data) can be found in Appendix B.

Surveillance and CHIS

Any officer who undertakes investigations (applicant) 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 CHIS.

The Council`s list of current officers who would undertake investigations and as such would be considered the case investigating officers are listed in Appendix B. It would be these officers who would attend the magistrate's court for the purpose of presenting RIPA cases to Justices of the Peace (JP) as it will be these officers who are best placed to answer any questions or clarify any points the JPs have on the application. However, the Authorising Officer's considerations should always be clearly and fully recorded on the application form, and in usual and complex cases consideration should be given to the Authorising Officer attending the court as well.

Each provisional authorisation then needs to receive judicial approval before being acted upon.

Communications Data

Any officer wishing to engage in conduct in relation to a postal service and telecommunication system for obtaining communications data and the disclosure to any person of such data must also seek authorisation, the procedure and procedure of which differs slightly and is outlined in paragraph 7.6.

7.2 Who can give the Stage 1 (Provisional) Authorisation?

By law, the 'Authorising Officer' for local authority purposes is a designated Director, Head of Service, service manager or equivalent. The Authorising Officer must ordinarily be independent from operations and investigations when granting authorisations related to those operations. In practice this means that an Authorising Officer should be far enough removed from the applicant's line management chain or the investigation so as not to be influenced by operational imperatives

An Authorising Officer may grant a provisional authorisation but it does not take effect until it receives judicial or OCDA approval.

The Council's Authorising Officer posts are listed in Appendix B. This appendix will be kept up to date by the Senior Responsible Officer as needs require. The Senior Responsible Officer has the delegated authority to add, delete or substitute posts.

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, or approved by the Senior Responsible Officer, before Authorising Officers are certified to sign any RIPA forms.

Central records of those individuals who have undergone RIPA training will be kept by the Senior Responsible Officer.

7.3 Grounds for Authorisation (the necessary and proportionate test)

An Authorising Officer has a number of obligations within the provisions of the Acts, which must be met before using any of the Investigatory powers.

An Authorising Officer shall not grant a provisional authorisation for the use of the RIPA powers 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 for surveillance and CHIS is deemed "**necessary**" in the circumstances of the particular case if it is for the purpose of the **prevention or detection of crime(s) punishable by 6 months imprisonment or more**, or relates to the sale of alcohol or tobacco to underage persons, and if that objective could not be achieved without the information sought.

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 and whether it could be punishable on summary conviction or on indictment, by a maximum term of at least six months imprisonment (surveillance and CHIS authorisations).

Careful consideration needs to be made by authorising officers of all of these points using the list below:

(a) is the size and scope of the operation balanced by the gravity and extent of the perceived crime or offence?

(b) is it clear how and why the methods to be adopted will cause the least possible intrusion on the subject and others?

(c) is the activity an appropriate use of the legislation and the only reasonable way, having considered all alternatives, of obtaining the necessary result?

(d) has evidence been provided of other methods considered and why they were not implemented?

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.

So far as possible, Authorising Officers should not be responsible for authorising investigations or operations in which they are directly involved.

7.4 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 use of the RIPA powers.

Where an operation unexpectedly interferes with the privacy of individuals who were not the subject of the investigation or covered by the authorisation in some other way, the investigating officer should inform the Authorising Officer.

7.5 Stage 2 – Judicial Approval (Surveillance and CHIS)

The judicial approval mechanism is in addition to the existing authorisation process under the relevant parts of RIPA as outlined in the Codes of Practice. The current local authority process of assessing necessity and proportionality, completing the RIPA authorisation / application form and seeking approval from an authorising officer will remain the same.

The Council is only able to grant a "provisional" authorisation or renewal to make use of any of the RIPA powers. All provisional authorisations and renewals must be approved by the Magistrates Court before the use of the RIPA power in the investigation commences.

The Council must apply to the local Magistrates Court for judicial approval of an authorisation or a renewal of an authorisation. 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.

An additional procedure note on '**How to apply to the Magistrate's Court for RIPA Approval'** has been produced which lays out the local arrangements in place and format of the court application.

The local authority will provide the JP with a copy of the original RIPA provisional authorisation or notice and the supporting documents setting out the case. This forms the basis of the application to the JP and **should contain all the information that is relied upon**.

The local authority will provide the JP with a partially completed judicial application form containing a brief summary of the circumstances of the case. This is supplementary to and does not replace the need to supply the provisionally authorised RIPA authorisation or renewal as well.

The Magistrates will consider the provisionally authorised application or renewal, and will need to satisfy themselves 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 applicant in liaison with legal services is responsible for tabling the application IN WRITING for judicial approval in the Magistrates Court before the use of the RIPA powers commence. The order section of the application form will be completed by the JP and will be the official record of the JP`s decision. The local authority will need to obtain judicial approval for all initial RIPA authorisations / applications and renewals and the local authority will need to retain a copy of the judicial application order form after it has been signed by the JP. There is no need for the JP to consider either cancellations or internal reviews.

The hearing is a 'legal proceeding' and therefore the local authority officers need to be formally designated to appear and present evidence or provide information as required by the JP. It will be the case investigator officers (identified in Appendix B) who will fulfil this role.

7.6 Special Procedure for Communications Data

The Data Retention and Investigatory Powers Act 2014 (DRIPA) and subsequently the Investigatory Powers Act 2016 remove the authority of accredited Council Officers to directly approach telecommunication service providers to obtain data under RIPA.

The introduction of the Office for Communications Data Authorisations (**OCDA**) means the acquisition of Communications Data by local authority officers is no longer subject to judicial approval by a Magistrate. OCDA assesses Communications Data applications from public authorities and makes decisions about those applications that strike a fine balance between the protection of privacy and the risk to public safety. OCDA acts as a hub of authorisation expertise, independently assessing applications, holding authorities accountable to robust safeguarding standards and challenging where required.

Applications for the obtaining and disclosure of communications data can now only be made through the National Anti-Fraud Network (NAFN) via their secure website (www.nafn.gov.uk). Reference should be made to the process map at **Appendix D** for guidance as to the process to be followed.

It is the responsibility of Fareham Borough Council to obtain provisional authorisation of an application by an authorising officer and then submit it to NAFN. However, NAFN will carry out the Single Point of Contact "**SPoC**" role which includes:

a) provide quality assurance checks to ensure that applications consistently comply with IPA standards and to a sufficient level to meet OCDA and IPCO scrutiny
b) monitor those applications which are returned for rework or rejected by OCDA and determine the reasons why
c) provide organisational and/or individual training as and where necessary sharing best practice, advice and support
d) be the point of contact between public authorities and OCDA

Applications to obtain communications data should be made on the interim form at Appendix D and submitted in the first instance to the Authorising Officer for feedback. This summary should be used as a record for the Central Monitoring records.

The formal application should then be entered on the NAFN website where it will be provisionally reviewed by a NAFN SPOC before forwarding to an Authorising Officer (Approved rank) set up on within the website. If satisfied that the proposed investigation is both necessary and proportionate, the Authorising Officer will complete the relevant parts of the application form. The relevant documents will then be retrieved from the NAFN application for presentation to the Office of Communications Data Authorisation (ODCA) who will issue a decision document. If accepted the NAFN application will be updated with the approval information. Any communications data obtained will be provided through the NAFN website.

Communications data, and all copies, extracts and summaries of it must be handled and stored securely. The requirements of the Data Protection Act 2018 and the principles of the Criminal Procedure and Investigations Act 1996 must be strictly followed.

Journalistic source

Where the purpose of a Communications Data application is to identify a journalistic source, these must first be authorized by an Authorising Individual (OCDA AO or DSO) but must also be approved by an IPCO Judicial Commissioner (JC). The Applicant and SPOC should pay special consideration to these applications and inform their Senior Responsible Officer. The IPA does not alter the existing processes for Communications Data applications that may feature sensitive professions including medical doctors, lawyers, journalists, parliamentarians or ministers of religion. If the Communications Data could contain information relating to any of these professions, this must be noted in the application.

7.7 Urgency

Urgent authorisation authorisations are no longer available in relation to the use of the RIPA powers.

7.8 Authorisation Forms

All authorisations must be in writing.

The local authority will provide the JP with a partially completed judicial application form that will also contain a brief summary of the circumstances of the case. This is supplementary to and does not replace the need to supply the provisionally authorised RIPA authorisation or renewal as well.

Standard forms for seeking use of the RIPA powers are provided at Appendix E. The authorisation shall be sought using the standard forms as amended from time to time.

8: JOINT AND OTHER INVESTIGATIONS

8.1 Activities by Other Public Authorities

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.

8.2 Joint Investigations

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

When some other agency (e.g. police, Customs & Excise, Inland Revenue etc):

(a) wish to use the Council's resources (e.g. CCTV surveillance systems), that agency must use its own RIPA procedures and, before any officer agrees to allow the Council's resources to be used for the other agency's purposes, he must obtain the details and purpose of the surveillance and evidence of the RIPA authorisation and any required judicial approval 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.

9: DURATION, RENEWAL AND CANCELLATION OF AUTHORISATIONS

9.1 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
(b) three months less a day from the date of the last judicial approval for directed surveillance
(c) one month from the date of judicial approval for communications data, or earlier if cancelled under Section 23(8) of the Act.

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

9.2 Reviews

The Authorising Officer shall undertake regular reviews of authorisations to assess the need for the surveillance to continue. At a minimum these should be carried out monthly from the start date. 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 E.

9.3 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 E.

9.4 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. The duty to cancel a notice falls on the authorising officer who issued it.

In the case of a notice issued in respect of communications data, the relevant postal or telecommunications operator will be informed of the cancellation.

Standard cancellation forms for communications data, directed surveillance and CHIS are attached at Appendix E.

When completing the cancellation form care should be taken to record when the activity ceased, what value the surveillance had been to the investigation and what evidence “products” had been obtained.

10: CORPORATE RECORDS

10.1 Types of Record

The Council must keep a detailed record of all provisional and judicially approved authorisations, reviews, renewals, cancellations and rejections in departments and a Central Register of all such forms will be maintained and contain the following information:

(a) a central register reference number for each authorisation

(b) a unique reference number for the authorisation (URN) - this is usually the investigation or operation case reference

(c) the type of authorisation or notice

(d) the date the provisional authorisation or notice was given;

(e) name and rank/grade of the authorising officer;

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

(g) whether the provisional authorisation was granted by an individual directly involved in the investigation;

(h) the date that judicial approval was received or refused;

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

(j) the date the authorisation or notice was cancelled;

(k) the outcomes of the use of the powers.

The title of the investigation or operation, including a brief description and names of subjects will only be recorded on the central register by way of a hyperlink to the application form. The content of the hyperlink is restricted and can only be accessed by those with the appropriate authority.

The record will be made available to inspectors from the Investigatory Powers Commissioner (IPCO) and retained to allow the Investigatory Powers Tribunal to carry out its functions. Records must be kept by the Council in accordance with the Communications Data Code of Practice and any relevant Guidance issued by the Investigatory Powers Commissioner. These records will be retained for a period of at least 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.

10.2 The Central Register

The Senior Responsible Officer shall hold and monitor the centrally retrievable record of all provisional and judicially approved authorisations. This can be found using the following path for the required year:

HUB\Corporate\RIPA\f. FBC CENTRAL MONITORING RECORDS\RIPA Central Record

Applicants and Authorising Officers are responsible for filling out the Central register for each application whether approved or not within 1 week of the judicial approval review, cancellation or rejection. They should also ensure that a copy of all applications, magistrates approvals, reviews, renewals and cancellation forms are saved to their central area on the network (under **k. COMPLETED FORMS**) and hyperlinked into the Central Register.

Once an authorisation has been cancelled the applicant or authorising officer must update the Central Register for the outcome of the use of the RIPA powers in relation to their investigation.

10.3 Records maintained in the Department

The Authorising Officer shall maintain the following documentation, which need not form part of the centrally retrievable record:

(a) the original signed application and a copy of the provisional authorisation or notice if applicable together with a copy of any order of judicial approval or refusal, as well as any supplementary documentation and notification 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) an original signed record of the result of each review of the authorisation or notice;
(e) the original signed renewal of an authorisation or notice, together with the supporting documentation submitted when the renewal was requested;
(f) the date and time when any instruction was given by the Authorising Officer.

Each form must have a URN and a Central Register number. The cross-referencing of each URN takes place within the form for audit purposes. Rejected forms will also have URNs.

10.4 Other Records for CHIS

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.

11: RETENTION AND DESTRUCTION

Material obtained from properly authorised surveillance or a source may be used in other investigations. Arrangements shall be in place for the handling, storage and destruction of material obtained through the use of covert surveillance, a source or the obtaining or disclosure of communications data. Authorising Officers must ensure compliance with the appropriate data protection requirements and any relevant Corporate Procedures relating to the handling and storage of material.

Where the product of surveillance could be relevant to pending or future proceedings, it should be retained in accordance with established disclosure requirements for a suitable period and subject to review.

12: SCRUTINY OF INVESTIGATORY BODIES

The **Investigatory Powers Commissioner's (IPCO)** has been established under RIPA 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 www.ipco.org.uk .

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 expects its officers to co-operate fully with these bodies and to bring forward any proposals for improvement that may follow on from an inspection report or a Tribunal hearing

APPENDIX A

GLOSSARY

Approved Rank

A recognised authorising officer in relation to Communications data.

CHIS

A person is a Covert Human Intelligence source if :

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

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

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

Communication

This refers to information transmission by post, email, phone, or internet provider.

Communication Data

This includes the ‘who’, ‘when’, ‘where’ and ‘how’ of a communication but not the content, i.e. what was said or written.

Confidential Material

Confidential information consists of matters subject to legal privilege, confidential personal information, confidential journalistic material and communications between an MP and a constituent.

Controller

A controller is someone assigned to be responsible for the management and supervision of a “handler” and general oversight of the use of the CHIS.

Handler

A handler is someone assigned to the day to day management of a CHIS.

IPCO

The Information Powers Commissioner’s Office is the national body that oversees the use of investigatory powers in RIPA.

OCDA

The Office for Communications Data Authorisations assesses and decides on communication data applications from public authorities.

RIPA Co-ordinator

This is a role recognised at Fareham Borough Council to support the Senior Responsible Officer role to maintain appropriate processes that comply with the law and codes of practice.

Senior Responsible Officer

This is the Officer of the Council appointed to ensure the integrity of processes within the Council and its compliance with RIPA. The current officer designated to this role is given in Appendix B.

Surveillance

'Surveillance' includes:

(a) monitoring, observing or listening to persons, their movements, their conversations or their other activities or communication;

(b) recording anything monitored, observed or listened to in the course of surveillance; and

(c) surveillance by or with the assistance of a surveillance device.

Surveillance also includes the interception of postal and telephone communications where the sender or recipient consents to the reading of or listening to or recording of the communication. This is a form of directed surveillance.

Telecommunications Operator

This is a person who offers or provides a communications service to persons in the UK, or controls or provides a communication system which is wholly or partly in the UK or controlled from the UK. This was previously known as the Communication Service Provider (CSP).

APPENDIX B

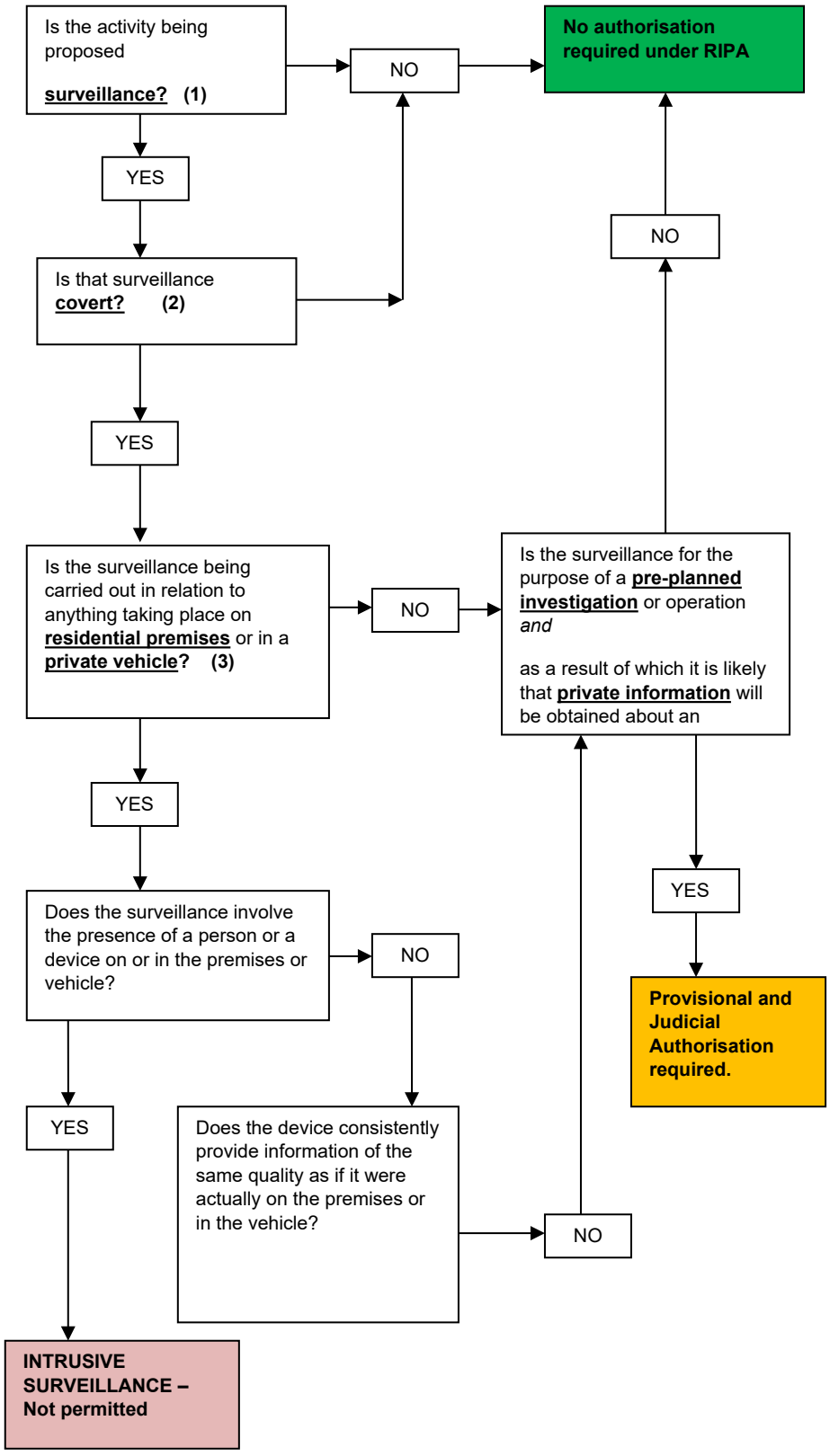
OFFICER APPOINTMENTS TO ROLES IN THE POLICY

Last reviewed June 2024

Title	Appointed Officers	Role
Senior Responsible Officer	Assistant Director (Finance and ICT) Elaine Hammell	Ensure the integrity of the process within the Council and its compliance with RIPA, including carrying out a periodic sample check of the quality of RIPA authorisations, renewals and cancellations. Carry out an annual review of the corporate policy. Have oversight of the completion of annual returns to the relevant oversight commissioner. Engage with the oversight commissioners when they conduct their inspections and where necessary, oversee the implementation of any post-inspection action plan. Have oversight of reporting of errors to the relevant oversight commissioner Ensure that Members regularly review the Council's use of RIPA. Nominate Approved Ranks for Communications Data Authorise request for excess data Maintain central records of individuals undertaken training.
RIPA Co-Ordinator	Audit Manager Clare Rogers	Monitoring day-to-day activity conducted under the Act. Carry out a periodic review of forms that are open for a long time or need a cancellation form completing, and will identify any links from forms to the Central Register that are missing Completion of annual returns to the relevant oversight commissioner. Lead on supporting the oversight commissioners when they conduct their inspections.
Authorising Officer (Surveillance/ CHIS) **Approved Rank (Communications Data)**	Neil Wood Abi Travers Adrian Collier Andrea Kingston Elaine Hammell Sarah Robinson Andrew Wannell	Review applications for considerations of: lawfulness, necessity, proportionality, collateral intrusion and approve or reject them. Act as applicant/handler as long as a different authorising officer approves the application.

Title	Appointed Officers	Role
Higher level authoriser **Designated Senior Officer (Comms Data)**	Andrew Wannell Sarah Robinson	Approve applications involving confidential material (surveillance) or the use of vulnerable individuals and juvenile sources (CHIS) Communications Data approval for emergency or life at risk
Applicant (Surveillance, Communications Data) **Handler (CHIS)**	Ian Smith Shohum Dave Clare Rogers	Complete application forms 1-4 (surveillance, CHIS) Complete NAFN Communications Data application Attend magistrates court to obtain judicial approval

DIRECTED SURVEILLANCE FLOW CHART



(1) Surveillance includes: monitoring, observing, listening to persons, their movements, their conversations or their other activities or communications. It includes recording anything monitored, observed or listened to in the course of surveillance, and surveillance by or with the assistance of a surveillance device

(2) Covert is defined as surveillance which is carried out in a manner calculated to ensure that the person(s) who are subject to it are unaware that it is or may be taking place

(3) Residential premises: occupied or used by a person, however temporarily, for residential purposes or otherwise as living accommodation including hotel rooms – but not communal areas – e.g. a hotel lounge.

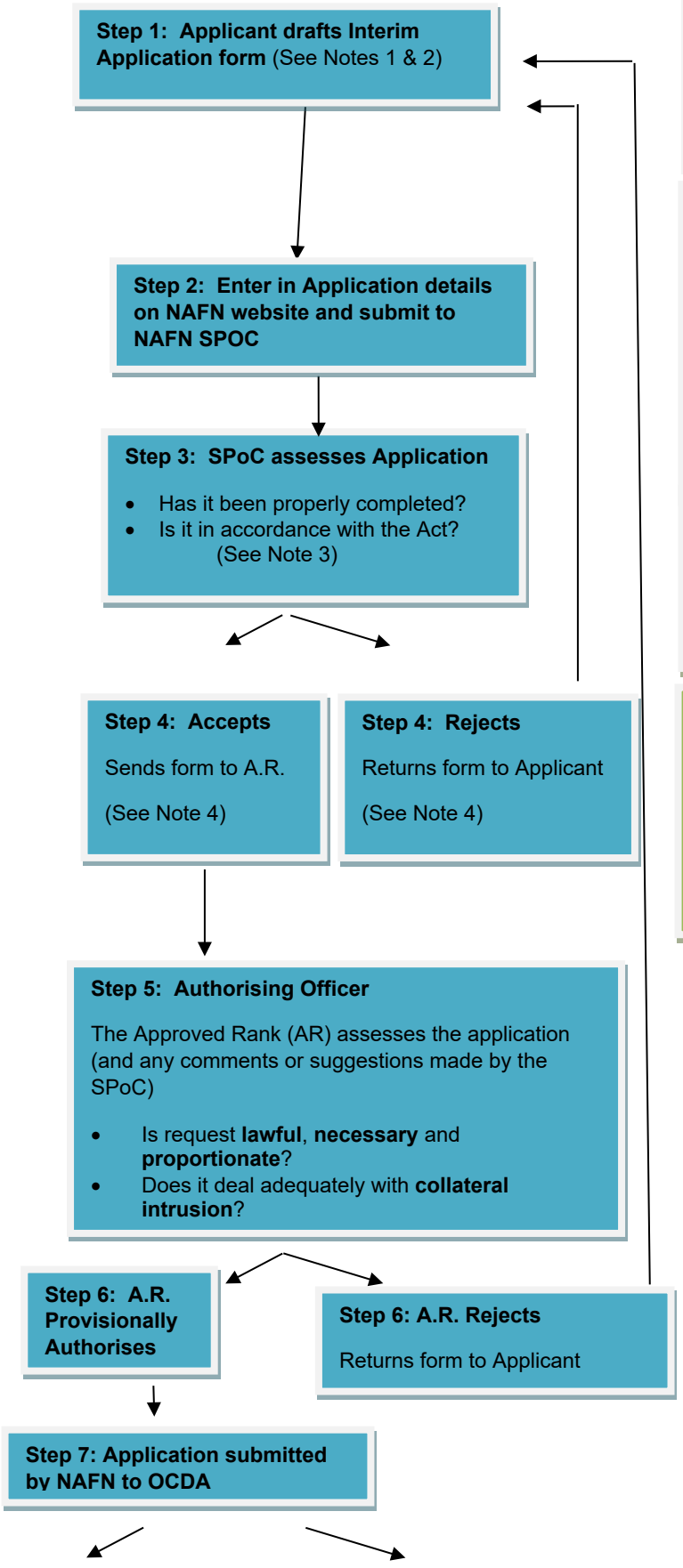
Private vehicle: which is used primarily for the private purpose of the owner or a person having the right to use it – but not, e.g. a minicab.

(4) Pre-planned investigation: surveillance is not planned if it is conducted as an immediate response to events or circumstances the nature of which it would not be reasonably practicable for authority to be sought.

Private information: includes any information relating to a person's private or family life. This must be interpreted broadly to include an individual's relationship with others. It will include information about a person's associations, lifestyle, finances etc. It is immaterial whether the person about whom the information will be gathered is the subject of the investigation.

Note: Before provisionally authorising any directed surveillance investigation, the Authorising Officer (AO) must clearly indicate in the authorisation form itself that the AO does believe that the proposed investigation is both **necessary** for preventing or detecting crime or preventing disorder **and** that the investigation is **proportionate** to what it is sought to achieve. The AO must also show that any potential **collateral intrusion** has been taken into account and that reasonable steps are proposed to minimise such intrusion.

COMMUNICATIONS DATA WORK FLOW



Note 1 Applicant should discuss proposed application with line manager to try to find alternative options for obtaining the information required.

Applicant may also wish to discuss content, scope and aims of the application and type of application with the NAFN SPoC before submitting the application

Note 2 The application should include:

- The statutory and case purpose for which the data is required
- Details of the offences being investigated
- A justification for the seriousness of the offence
- The nature of the enquiry
- Details of the data required
- The timescale in which the data is needed
- A statement clearly setting out:
  - why request is **necessary**
  - why request is **proportionate**
  - steps to be taken to minimise **collateral intrusion**

Note 3 The SPoC will:

- ensure application is practical and lawful, including purpose is permitted
- advice on most appropriate route to satisfy applicants needs
- assess cost and resource implications

Note 4 If the SPoC **accepts** that the application is justified and reasonably practicable, s/he:

- will submit the application to the AR for approval
- include any appropriate additional information/comments for consideration by AR

If the SPoC **rejects** the application, s/he will:

- return the application to the applicant
- specify in writing reason(s) for rejection

Note 5 If A.R. **authorises** the application, s/he will:

- Approve online
- document any discussions conducted in reaching the decision

If A.R **rejects** the application, s/he will:

- return the application to the applicant
- specify in writing reason(s) for rejection

KEY

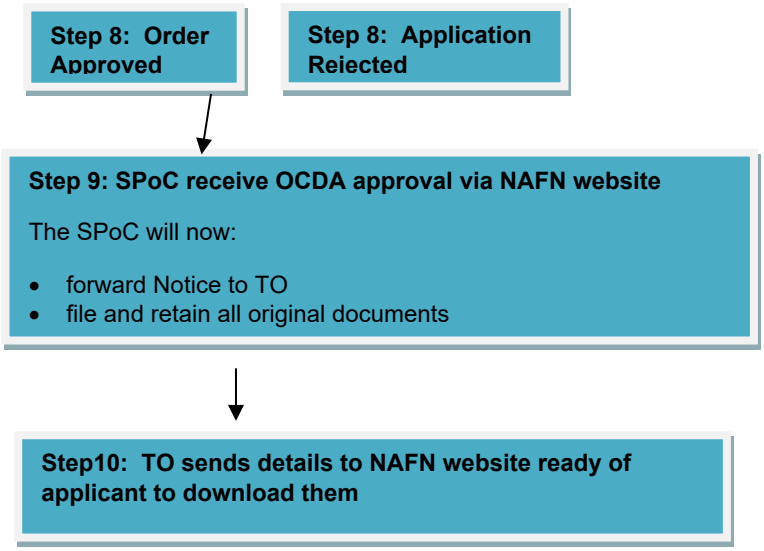
Applicant: *Officer making the application*

A.R.: *Approved Rank who provisionally authorises the Application*

SPoC: *Single Point of Contact between FBC and TO*

OCDA: *Office of Communications Data Authorisations*

TO: *Telecommunications Provider*


Step 8: Order Approved
Step 8: Application Rejected
Step 9: SPoC receive OCDA approval via NAFN website
The SPoC will now:
• forward Notice to TO
• file and retain all original documents
Step10: TO sends details to NAFN website ready of applicant to download them

APPENDIX E

RIPA FORMS

The following links can be used to locate the template of the latest forms to use which are stored on the Hub at: Corporate\RIPA\b. FBC RIPA FORMS

Directed Surveillance

a. Directed Surveillance Authorisation - RIPA 1
b. Directed Surveillance Review - RIPA 2
c. Directed Surveillance Renewal - RIPA 3
d. Directed Surveillance Cancellation - RIPA 4

Covert Human Intelligence (CHIS)

a. CHIS Application - CHIS 1
b. CHIS Review - CHIS 2
c. CHIS Renewal - CHIS 3
d. CHIS Cancellation - CHIS 4

Application for judicial approval to obtain or disclose communications data, to use covert human intelligence source or to conduct directed surveillance

Judicial Approval Application Form

Accompanying Witness Statement

Communications Data

Template to prepare for application via NAFN

Link to National Anti-Fraud Network site - https://secure.nafn.gov.uk/