Reigate & Banstead Borough Council
Regulation of Investigatory Powers Act 2000 (RIPA) corporate policy and procedures

Use of directed surveillance covert human intelligence sources and communications data acquisition for the prevention and detection of crime or the prevention of disorder

Reigate & Banstead
BOROUGH COUNCIL
Banstead | Horley | Redhill | Reigate

Version control sheet

Title:	RIPA Policy.
Purpose:	To advise staff of the procedures and principles to follow to comply with the RIPA Act.
Author:	Michaela Lambart – Fraud Manager
Owner:	Simon Rosser – Head of Revenues, Benefits and Fraud.
Approved by	Mari Roberts-Wood
Date:	**July 2020**
Date Amended:	**04th August 2020**
Version number:	Issue 2
Status:	Final.
Review frequency:	Bi-Annually.
Reviewed:	**July 2022**
Next review date:	**July 2024**

Contents

1. A brief overview of RIPA

The Regulation of Investigatory Powers Act (the Act) was introduced by Parliament in 2000. The Act sets out the reasons for which the use of **directed surveillance** (DS) and **covert human intelligence source** (CHIS) may be authorised.

Local Authorities' abilities to use these investigation methods are restricted in nature and may only be used for the prevention and detection of crime or the prevention of disorder. Local Authorities are not able to use **intrusive surveillance**.

Widespread, and often misinformed, reporting led to public criticism of the use of surveillance by some Local Authority enforcement officers and investigators. Concerns were also raised about the trivial nature of some of the 'crimes' being investigated. This led to a review of the legislation and ultimately the introduction of the Protection of Freedoms Act 2012 and the RIPA (Directed Surveillance and CHIS) (Amendment) Order 2012 (Appendix 2).

In addition to defining the circumstances when these investigation methods may be used, the Act also directs how applications will be made and how, and by whom, they may be approved, reviewed, renewed, cancelled and retained.

The Act must be considered in tandem with associated legislation including the Human Rights Act (HRA) (Appendix 2), and the Data Protection Act (DPA) (Appendix 2).

The purpose of Part II of the Act is to protect the privacy rights of anyone in a Council's area, but only to the extent that those rights are protected by the HRA. A public authority, such as the Council, can infringe those rights provided that it does so in accordance with the rules, which are contained within Part II of the Act. Should the public authority not follow the rules, the authority loses the impunity otherwise available to it. This impunity may be a defence to a claim for damages or a complaint to supervisory bodies, or as an answer to a challenge to the admissibility of evidence in a trial.

Further, a Local Authority may only engage the Act when performing its 'core functions'. For example, a Local Authority may rely on the Act when conducting a criminal investigation as this would be considered a 'core function', whereas the disciplining of an employee would be considered a 'non-core' or 'ordinary' function.
Examples of when local authorities may use RIPA and CHIS are as follows:

- Enforcement of anti-social behaviour orders and legislation relating to unlawful child labour;
- Housing/planning – interventions to stop and make remedial action against unregulated and unsafe buildings, breaches of preservation orders, cases of landlord harassment;
- Counter Fraud – investigating allegations of fraud, bribery, corruption and theft committed against the Council; and
- Environment protection – action to stop large-scale waste dumping, the sale of unfit food and illegal 'raves'.

The examples do not replace the key principles of necessity and proportionality or the advice and guidance available from the relevant oversight Commissioners.

The RIPA (Communications Data) order came into force in 2004. It allows Local Authorities to acquire communications data, namely service data and subscriber details for limited purposes.

The Investigatory Powers Act 2016 (IPA) came into force for local authorities on Tuesday 11 June 2019. The IPA is the main legislation governing the acquisition of communications data. It brings together relevant powers but does not fully replace pre-existing legislation.

2. Directed surveillance

This policy relates to all staff directly employed by RBBC when conducting relevant investigations for the purposes of preventing and detecting crime or preventing disorder, and to all contractors and external agencies that may be used for this purpose as well as to those members of staff tasked with the authorisation and monitoring of the use of directed surveillance, CHIS and the acquisition of communications data.

The policy will be reviewed bi-annually and whenever changes are made to relevant legislation and codes of practice.

The use of directed surveillance or a CHIS must be necessary and proportionate to the alleged crime or disorder. Usually, it will be a tool of last resort, to be used only when all other less intrusive lines of enquiry have been used or considered.

Necessary & Proportionate

A person granting an authorisation for directed surveillance must consider why it is necessary to use covert surveillance in the investigation and believe that the activities to be authorised are necessary on one or more statutory grounds.

If the activities are deemed necessary, the authoriser must also believe that they are proportionate to what is being sought to be achieved by carrying them out. This involves balancing the seriousness of the intrusion into the privacy of the subject of the operation (or any other person who may be affected) against the need for the activity in investigative and operational terms.

The authorisation will not be proportionate if it is excessive in the overall circumstances of the case. Each action authorised should bring an expected benefit to the investigation or operation and should not be disproportionate or arbitrary. The fact that a suspected offence may be serious will not alone render intrusive actions proportionate. Similarly, an offence may be so minor that any deployment of covert techniques would be disproportionate. No activity should be considered proportionate if the information which is sought could reasonably be obtained by other less intrusive means.

The following elements of proportionality should therefore be considered:

- balancing the size and scope of the proposed activity against the gravity and extent of the perceived crime or offence
- explaining how and why the methods to be adopted will cause the least possible intrusion on the subject and others
- considering whether the activity is an appropriate use of the legislation and a reasonable way, having considered all reasonable alternatives, of obtaining the necessary result
- evidencing, as far as reasonably practicable, what other methods had been considered and why they were not implemented

The Council will conduct its directed surveillance operations in strict compliance with the DPA principles and limit them to the exceptions permitted by the HRA and RIPA, and solely for the purposes of preventing and detecting crime or preventing disorder.

The **Senior Responsible Officer** (SRO) (as named in Appendix 3) will be able to give advice and guidance on this legislation. The SRO will appoint a **RIPA Coordinating Officer** (RCO) (as named in Appendix 3) The RCO will be responsible for the maintenance of a **central register** that will be available for inspection by the Office of the Surveillance Commissioners (OSC). The format of the central register is set out in Appendix 4.

The use of hand-held cameras and binoculars can greatly assist a directed surveillance operation in public places. However, if they afford the investigator a view into private premises that would not be possible with the naked eye, the surveillance becomes intrusive and is not permitted. Directed surveillance may be conducted from private premises. If they are used, the applicant must obtain the owner's permission, in writing, before authorisation is given. If a prosecution then ensues, the applicant's line manager must visit the owner to discuss the implications and obtain written authority for the evidence to be used.

The general usage of the council's CCTV system is not affected by this policy. However, if cameras are specifically targeted for the purpose of directed surveillance, a RIPA authorisation must be obtained.

Wherever knowledge of **confidential information** is likely to be acquired or if a vulnerable person or juvenile is to be used as a CHIS, the authorisation must be made by the Chief Executive, who is the Managing Director (or in their absence whoever deputises for this role).

Directed surveillance that is carried out in relation to a **legal consultation** on certain premises will be treated as intrusive surveillance, regardless of whether legal privilege applies or not. These premises include prisons, police stations, courts, tribunals and the premises of a professional legal advisor. Local Authorities are not able to use intrusive surveillance. Operations will only be authorised when there is enough, documented, evidence that the alleged crime or disorder exists and when directed surveillance is considered to be a necessary and proportionate step to take in order to secure further evidence.

Low level surveillance, such as 'drive-bys' or everyday activity observed by officers in the course of their normal duties in public places, does not need RIPA authority. If surveillance activity is conducted in immediate response to an unforeseen activity, RIPA authorisation is not required.
However, if repeated visits are made for a specific purpose, authorisation may be required. In cases of doubt, legal advice should be taken.

When vehicles are being used for directed surveillance purposes, drivers must always comply with relevant traffic legislation.

Crime threshold

An additional barrier to authorising directed surveillance is set out in the Regulation of Investigatory Powers (Directed Surveillance and CHIS) (Amendment) Order 2012. This provides a 'Crime Threshold' whereby only crimes which are either punishable by a minimum term of at least 6 months' imprisonment (whether on summary conviction or indictment) or are related to the underage sale of alcohol or tobacco can be investigated through Directed Surveillance.

The crime threshold applies only to the authorisation of directed surveillance by local authorities under RIPA, not to the authorisation of local authority use of CHIS or their acquisition of Communications Data. The threshold came into effect on 1 November 2012.

RBBC 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 minimum term of at least 6 months' imprisonment.

RBBC may therefore continue to authorise use of directed surveillance in more serious cases if the other tests are met – i.e. that it is necessary and proportionate and where prior approval from a Magistrate has been granted. Examples of cases where the offence being investigated attracts a minimal custodial sentence of six months or more could include more serious criminal damage, dangerous waste dumping and serious or serial fraud.

RBBC may also continue to authorise the use of directed surveillance for the purpose of preventing or detecting specified criminal offences relating to the underage sale of alcohol and tobacco where the necessity and proportionality test is met and prior approval from a Magistrate has been granted.

A local authority such as RBBC may not authorise the use of directed surveillance under RIPA to investigate disorder that does not involve criminal offences.

3. Covert Human Intelligence Sources (CHIS)

A person who reports suspicion of an offence is not a CHIS, nor do they become a CHIS if they are asked if they can provide additional information, e.g. details of the suspect's vehicle or the time that they leave for work. It is only if they establish or maintain a personal relationship with another person for the purpose of covertly obtaining or disclosing information that they become a CHIS.

The times when a local authority will use a CHIS are carefully considered depending on the investigation taking place. The usage for test purchasing will always take place under the supervision of suitably trained officers.

The processes for applications and authorisations have similarities to those for directed surveillance but there are also significant differences, namely that the following arrangements must always be in place in relation to the use of a CHIS:

- There will be an appropriate officer of the Council who has day-to-day responsibility for dealing with the CHIS, and for the security and welfare of the CHIS; and
- There will be a second appropriate officer of the use made of the CHIS, and who will have responsibility for maintaining a record of this use. These records must also include information prescribed by the Regulation of Investigatory Powers (Source Records)
- Regulations 2000. Any records that disclose the identity of the CHIS must not be available to anyone who does not have a need to access these records.

4. The authorisation process

Directed Surveillance applications and CHIS applications are made using forms available on the home office website. These forms must not be amended, and applications will not be accepted if the approved forms are not completed. A new form for each new case should be downloaded from the Home Office Website every time to ensure correct form is in use.

The authorisation process involves the following steps:

Investigation Officer

A risk assessment will be conducted by the Investigation Officer before an application is drafted and prior to staff being deployed. Lone workers will not undertake surveillance, unless this has been carefully considered and is appropriate to the investigation. This assessment will include the number of officers required for the operation; whether the area involved is suitable for directed surveillance; what equipment might be necessary, health and safety concerns of all those involved and affected by the operation and insurance issues.

Care must be taken when considering surveillance activity close to schools or in other sensitive areas. If it is necessary to conduct surveillance around school premises, the applicant should inform the head teacher of the nature and duration of the proposed activity, in advance. A Police National Crime database check on those targets should be conducted as part of this assessment by the Counter Fraud & Investigation team. The risk assessment and any notification to a head teacher will be recorded on the case file.

The Investigation Officer prepares an application. When completing the forms, Investigation Officers must fully set out details of the covert activity for which authorisation is sought to enable the Authorising Officer to make an informed judgment. Consideration should be given to consultation with a lawyer concerning the activity to be undertaken (including scripting and tasking).

The Investigation Officer will obtain a unique reference number (URN) from the central register, maintained by the **RIPA Co-ordinating Officer (RCO**) before submitting an application.

The Investigation Officer will submit the application form to an authorising officer for approval (see Appendix 5).

All applications to conduct directed surveillance (other than under urgency provisions – see below) must be made in writing in the approved format.

Authorising Officer (AO)

The AO considers the application and if it is considered complete the application is signed off and forwarded to the SRO for review and counter approval.

If there are any deficiencies in the application further information may be sought from the Investigation Officer, prior to sign off.

Once final approval has been received from the SRO (see below), the AO and the Investigation Officer will retain copies and will create an appropriate diary method to ensure that any additional documents are submitted in good time.

Senior Responsible Officer (SRO)

The SRO or their deputy then reviews the AO's approval and countersigns it.

If the application requires amendment the SRO or their deputy will return this to the AO for the necessary revisions to be made prior to sign off. Once the SRO or their deputy is satisfied that concludes the internal authorisation procedure and he or she will countersign the application.

Once the SRO has countersigned the form this will form the basis of the application to the Magistrates Court for authorisation

Application to Magistrates Court

The countersigned application form will form the basis of the application to the Magistrates court

Authorised activity

Authorisation takes effect from the date and time of the approval from the Magistrates court.

Where possible, private vehicles used for directed surveillance purposes should have keeper details blocked by the Counter Fraud & Investigation team.

Notification of the operation will be made to the relevant police force intelligence units where the target of the operation is in their force area. Contact details for each force intelligence unit are held at Appendix 3

Before directed surveillance, activity commences, the Investigation Officer will brief all those taking part in the operation. The briefing will include details of the roles to be played by each officer, a summary of the alleged offence(s), the name and/or description of the subject of the directed surveillance (if known), a communications check, a plan for discontinuing the operation and an emergency rendezvous point.

Where 3 or more officers are involved in an operation, officers conducting directed surveillance will complete a daily log of activity an example shown at Appendix 5. Evidential notes will also be made in the pocket notebook of all officers engaged in the operation regardless of the number of officers on an operation. These documents will be kept in accordance with the appropriate retention guidelines and Criminal Procedure Investigation Act.

Where a contractor or external agency is employed to undertake any investigation on behalf of the Council, the Investigation Officer will ensure that any third party is adequately informed of the extent of the authorisation and how they should exercise their duties under that authorisation.

Conclusion of activities

As soon as the authorised activity has concluded the Investigation Officer will complete a Cancellation Form.

The original document of the complete application will be retained in the investigation file. A summary will be maintained in a central register.

5. Judicial authorisation

From 1 November 2012, sections 37 and 38 of the Protection of Freedoms Act 2012 are in force.

This will mean that a local authority who wishes to authorise the use of directed surveillance, acquisition of Communication Data (CD) and use of a CHIS under RIPA will need to obtain an order approving the grant or renewal of an authorisation or notice from a Magistrate before it can take effect. If the Magistrate is satisfied that the statutory tests have been met and that the use of the technique is necessary and proportionate, he/she will issue an order approving the grant or renewal for the use of the technique as described in the application.

The new judicial approval mechanism is in addition to the existing authorisation process under the relevant parts of RIPA as outlined above and in this section. The current process of assessing necessity and proportionality, completing the RIPA authorisation/application form and seeking approval from an authorising officer/designated person will therefore remain the same.

The appropriate officer from RBBC will provide the Magistrate with a copy of the original RIPA authorisation or notice and the supporting documents setting out the case. This forms the basis of the application to the Magistrate and should contain all information that is relied upon. For communications data requests the RIPA authorisation or notice may seek to acquire consequential acquisition of specific subscriber information. The necessity and proportionality of acquiring consequential acquisition will be assessed by the magistrate as part of their consideration.

The original RIPA authorisation or notice should be shown to the Magistrate but also will be retained by RBBC so that it is available for inspection by the Commissioners' officers and in the event of any legal challenge or investigations by the Investigatory Powers Tribunal (IPT). The
Court may also wish to keep a copy so an extra copy should be made available to the Court.
Importantly, the appropriate officer will also need to provide the Magistrate with a partially completed judicial application/order form.

Although the officer is required to provide a brief summary of the circumstances of the case on the judicial application form, this is supplementary to and does not replace the need to supply the original RIPA authorisation as well.

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

The authorisation will take effect from the date and time of the Magistrate granting approval and RBBC may proceed to use the techniques approved in that case.

It will be important for each officer seeking authorisation to establish contact with Her Majesty's Court and Tribunals Service (HMCTS) administration at the magistrates' court. HMCTS administration will be the first point of contact for the officer when seeking a Magistrates approval. RBBC will need to inform HMCTS administration as soon as possible to request a hearing for this stage of the authorisation.

On the rare occasions where out of hours access to a Magistrate is required then it will be for the officer to make local arrangements with the relevant HMCTS legal staff. In these cases we will need to provide two partially completed judicial application/order forms so that one can be retained by the Magistrate. They should provide the court with a copy of the signed judicial application/order form the next working day.

In most emergency situations where the police have power to act, then they can authorise activity under RIPA without prior Magistrate's approval. No RIPA authority is required in immediate response to events or situations where it is not reasonably practicable to obtain it (for instance when criminal activity is observed during routine duties and officers conceal themselves to observe what is happening).

Where renewals are timetabled to fall outside of court hours, for example during a holiday period, it is the local authority's responsibility to ensure that the renewal is completed ahead of the deadline. Out of hours procedures are for emergencies and should not be used because a renewal has not been processed in time.

The hearing is a 'legal proceeding' and therefore our officers need to be formally designated to appear, be sworn in and present evidence or provide information as required by the Magistrate.

The hearing will be in private and heard by a single Magistrate who will read and consider the RIPA authorisation or notice and the judicial application/order form. He/she may have questions to clarify points or require additional reassurance on matters.

The attending officer will need to be able to answer the Magistrate's questions on the policy and practice of conducting covert operations and the detail of the case itself. RBBC's officers may consider it appropriate for the RIPA Co-ordinating Officer to attend for applications for CD/RIPA authorisations. This does not, however, remove or reduce in any way the duty of the authorising officer to determine whether the tests of necessity and proportionality have been met. Similarly, it does not remove or reduce the need for the forms and supporting papers that the authorising officer has considered, and which are provided to the Magistrate to make the case.

It is not RBBC's policy that legally trained personnel are required to make the case to the Magistrate. The forms and supporting papers must by themselves make the case. It is not enough for the local authority to provide oral evidence where this is not reflected or supported in the papers provided. The Magistrate may note on the form any additional information he or she has received during the hearing but information fundamental to the case should not be submitted in this manner.

If more information is required to determine whether the authorisation or notice has met the tests, then the Magistrate will refuse the authorisation. If an application is refused, the local authority should consider whether they can reapply, for example, if there was information to support the application which was available to the local authority, but not included in the papers provided at the hearing.

The Magistrate will record his/her decision on the order section of the judicial application/order form.

HMCTS administration will retain a copy of the local authority RIPA authorisation or notice and the judicial application/order form. This information will be retained securely, Magistrates' Courts are not public authorities for the purposes of the Freedom of Information Act 2000.

RBBC will need to provide a copy of the order to the **RCO** for all Communications Data requests. **RCOs** must not acquire the Communications Data requested, until the application has been given Judicial Approval by a Magistrate

6 Authorisation periods

The authorisation will take effect from the date and time of the Magistrate granting approval and RBBC may proceed to use the techniques approved in that case. It is RBBC policy that all applications will have the duration stated at the point of application.

Urgent oral or written authorisations, unless renewed, cease to have effect after 72 hours, beginning with the time when the authorisation was granted.

Renewals should not normally be granted more than seven days before the original expiry date. If the circumstances described in the application alter, the applicant must submit a review document before activity continues.

As soon as the operation has obtained the information needed to prove, or disprove, the allegation, the applicant must submit a cancellation document and the authorised activity must cease.

CHIS authorisations will (unless renewed or cancelled) cease to have effect 12 months from the day on which authorisation took effect, except in the case of juvenile CHIS which will cease to have effect after 1 month.

7. Urgency

The law has been changed so that urgent cases can no longer be authorised orally. Approval for directed surveillance in an emergency must now be obtained in written form. Oral approvals are no longer permitted. In cases where emergency approval is required an AO must be visited by the applicant with two completed RIPA application forms. The AO will then assess the proportionality, necessity and legality of the application. If the application is approved, then the applicant must then contact the out-of-hours HMCTS representative to seek approval from a Magistrate. The applicant must then take two signed RIPA application forms and the judicial approval form to the Magistrate for the hearing to take place.

As with a standard application the test of necessity, proportionality and the crime threshold must be satisfied. A case is not normally to be regarded as urgent unless the delay would, in the judgment of the person giving the authorisation, be likely to endanger life or jeopardise the investigation or operation. Examples of situations where emergency authorisation may be sought would be where there is intelligence to suggest that there is a substantial risk that evidence may be lost, a person suspected of a crime is likely to abscond, further offences are likely to take place and/or assets are being dissipated in a criminal investigation and money laundering offences may be occurring. An authorisation is not considered urgent if the need for authorisation has been neglected or the urgency is due to the authorising officer or applicant's own doing.

8. Telecommunications data - NAFN

The RIPA (Communications Data) Order 2003 came into law in January 2004. The Investigatory Powers Act 2016 (IPA) came into force for local authorities on Tuesday 11 June 2019. It allows Local Authorities to acquire limited information in respect of subscriber details and service data. It does
NOT allow Local Authorities to intercept, record or otherwise monitor communications data.

Applications to use this legalisation must be submitted to a Home Office accredited Single Point of Contact (SPOC). The Council uses the services of NAFN (the National Anti-fraud Network) for this purpose.

Officers may make the application by accessing the NAFN website. The application will first be vetted by NAFN for consistency, before being forwarded by NAFN to the Council's Designated Persons for the purposes of approving the online application. The Council will ensure that
Designated Persons receive appropriate training when becoming a Designated Person.

The Council's Designated Persons are listed in Appendix 3. NAFN will inform the Designated Persons jointly once the application is ready to be reviewed by the Designated Persons.

The relevant Designated Persons responsible for the area to which the application relates, will then access the restricted area of the NAFN website using a special code, in order to review and approve the application. When approving the application, the Designated Person must be satisfied that the acquiring of the information is necessary and proportionate. Approvals are documented by the Designated Person completing the online document and resubmitting it by following the steps outlined on the site by NAFN. This online documentation is retained by NAFN who are inspected and audited by the Office Surveillance Commissioner (OSC).

When submitting an online application, the officer must also inform the relevant Designated Person, in order that they are aware that the NAFN application is pending.

9. Handling of material and use of material as evidence

Material obtained from properly authorised directed surveillance or a source may be used in other investigations. Arrangements shall be in place for the handling, storage and destruction of material obtained using directed surveillance, a source or the obtaining or disclosure of communications data, following relevant legislation such as the Criminal Procedure and
Investigations Act (CPIA). Authorising Officers must ensure compliance with the appropriate data protection and CPIA requirements, having due regard to the Public Interest Immunity test 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.

If the investigation leads to a prosecution and conviction, then the records should be retained for the duration of the sentence plus two years. If the investigation does not lead to a prosecution, then records should be retained for six years.

10. Training

"*It is essential that the Chief Executive, or Managing Director, together with the Directors and the Heads of Units should have an awareness of the basic requirements of RIPA and an understanding of how it might apply to the work of individual council departments. Without this knowledge at senior level, it is unlikely*

that any authority will be able to develop satisfactory systems to deal with the legislation. Those who need to use or conduct directed surveillance or
CHIS on a regular basis will require more detailed specialised training" (Office of Surveillance Commissioners).

Officers conducting directed surveillance operations, using a CHIS or acquiring communications data must have an appropriate accreditation or be otherwise suitably qualified or trained.

Authorising Officers (Appendix 3) will be appointed by the Chief Executive and will have received training that has been approved by the Senior Responsible Officer. The Senior Responsible
Officer will have appointed the RIPA Coordinating Officer and the Training Officer. (Appendix 3)

All training will take place at reasonable intervals to be determined by the Training Officer, but it is envisaged that an update will usually be necessary following legislative or good practice developments or otherwise every 2 years.

11. The inspection process

Investigatory Powers Commissioner's Office (IPCO) will make periodic inspections during which the inspector will wish to interview a sample of key personnel; examine RIPA and CHIS applications and authorisations; the central register and policy documents. The inspector will also make an evaluation of processes and procedures.

12. Resources

Full Codes of Practice can be found on the Home Office website:
http://www.homeoffice.gov.uk/

Covert Surveillance & Property Interference:
https://www.gov.uk/government/publications/code-of-practice-for-covert-surveillance-and-propertyinterference

CHIS:
https://www.gov.uk/government/publications/code-of-practice-for-the-use-of-human-intelligencesources

Acquisition and Disclosure of Communications Data:
https://www.gov.uk/government/publications/code-of-practice-for-the-acquisition-and-disclosure-ofcommunications-data

Further information can also be found on The IPCO website:
https://www.ipco.org.uk/

Appendix 1 - glossary of terms –

Collateral intrusion	The likelihood of obtaining private information about someone who is not the subject of the directed surveillance operation.
Confidential information	This covers confidential journalistic material, matters subject to legal privilege, and information relating to a person (living or dead) relating to their physical or mental health; spiritual counselling or which has been acquired or created in the course of a trade/profession/occupation or for the purposes of any paid/unpaid office.
Covert relationship	A relationship in which one side is unaware of the purpose for which the relationship is being conducted by the other.
Directed surveillance	Surveillance carried out in relation to a specific operation which is likely to result in obtaining private information about a person in a way that they are unaware that it is happening. It excludes surveillance of anything taking part in residential premises or in any private vehicle.
Intrusive surveillance	Surveillance which takes place on any residential premises or in any private vehicle. A Local Authority cannot use intrusive surveillance.
Legal consultation	A consultation between a professional legal adviser and his client or any person representing his client, or a consultation between a professional legal adviser or his client or representative and a medical practitioner made in relation to current or future legal proceedings.
Residential premises	Any premises occupied by any person as residential or living accommodation, excluding common areas to such premises, e.g. stairwells and communal entrance halls.
Senior Responsible Officer (SRO)	The SRO is responsible for the integrity of the processes for the Council to ensure compliance when using Directed Surveillance or CHIS.
Service data	Data held by a communications service provider relating to a customer's use of their service, including dates of provision of service; records of activity such as calls made, recorded delivery records and top-ups for pre-paid mobile phones.
Surveillance device	Anything designed or adapted for surveillance purposes.

Appendix 2 - Relevant Legislation

Regulation of Investigatory Powers (Directed Surveillance and Covert Human Intelligence Sources) Order 2010

The Order consolidates four previous Orders relating to directed surveillance and the use or conduct of covert human intelligence sources by public authorities under Part II of the Regulation of Investigatory Powers Act 2000 (RIPA) and to reflect the outcome of a public consultation which took place between April and July 2009.

It identifies the 'relevant public authorities' authorised to conduct RIPA and CHIS activities. This list includes local authorities in England and Wales. It also gives examples of such activity, as shown on page 3 of this document.

The Human Rights Act 1998

Articles 6 and 8 of the Human Rights Act are relevant to RIPA.

If it is proposed that directed surveillance evidence is to be used in a prosecution, or other form of sanction, the subject of the surveillance should be informed during an interview under caution.

The Data Protection Act 1998 (DPA)

The eight principles of the Act relating to the acquisition of personal data need to be observed when using RIPA. To ensure compliance, the information must:

- be fairly and lawfully obtained and processed
- be processed for specified purposes only
- be adequate, relevant and not excessive
- be accurate
- not be kept for longer than is necessary
- be processed in accordance with an individual's rights
- be secure
- not be transferred to non EEA countries without adequate protection

Appendix 3 – Roles and Responsibilities

Senior Responsible Officers & NAFN Designated Person: review Authorising Officers' approval and countersign, also approve the online application administered by NAFN

Pat Main Head of Finance	Senior Responsible Officer (SRO)	01737 276063
Mari Roberts- Wood Managing Director	Deputy Senior Responsible Officer	01737 276030

RIPA Co-ordinating Officer - maintains the central register and training record for the Council.

Michaela Lambart Fraud manager	RIPA Co-ordinating Officer	01737 276518

Fraud Manager – maintains the registration with NAFN and arranges training as required

Michaela Lambart	Fraud Manager	01737 276518

Authorising officers & NAFN Designated Persons – considers the application provided by the Investigating Officer and when appropriate approves the application, prior to consideration by the Senior Responsible Officer. Also approves the online application administered by NAFN

Mari Roberts- Wood Managing Director	Authorising Officer & NAFN Designated Person	01737 276030
Luci Mould Director of Place	Authorising Officer & NAFN Designated Person	01737 276214

Authorisation by Chief Executive

If a vulnerable person or juvenile is to be used as a CHIS, the authorisation must be made by the Managing Director: Mari Roberts-Woods or in her absence one of the following Director will be responsible: Luci Mould.

Training Officer

The RIPA Co-ordinating Officer will be responsible for arranging suitable training for those conducting surveillance activities, Senior Responsible Officers, Authorising Officers, NAFN Designated Persons and will ensure that a training record is maintained for the Council.

Investigating Officer – conducts a risk assessment, prepares the application form, obtains the unique reference number from the RIPA Co-originating Officer, maintains the case file and where appropriate completes the cancellation form.

Appendix 4 - central register

A central register will be maintained by the RIPA Co-ordinating Officer. The register will contain details of all RIPA and CHIS applications (whether approved or not) and all reviews, renewals and cancellations, together with a register of all training undertaken by anyone associated with RIPA at RBBC.

Each operation will be given a unique reference number (URN) from which the department involved, and the year of the operation may be readily identified.

The register will also contain the following information:

- the operation reference name or number
- the name of the applicant
- the name of the subject of the surveillance or CHIS activity (for internal enquiries a
- pseudonym may be used)
- the date and time that the activity was authorised
- the date and time of any reviews that are to be conducted
- the date and time of any renewals of authorisations
- the date and time of the cancellations of any authorisations

Kept in conjunction with the register will be the details of the training and updates delivered to authorising officers, a list of authorising officers, a copy of the RIPA policy and copies of all relevant legislation.

The original of all documents will also be held with the register, which must be available for inspection by the Office of the Surveillance Commissioners.

Appendix 5 - surveillance log

Daily log of activity to be kept by each operator or pair of operators.

A – Amount of time under observation

D – Distance from subject

V – Visibility

O – Obstruction

K – Known, or seen before

A – Any reason to remember, subject or incident

T – Time elapsed between sighting and note taking

E – Error or material discrepancy – e.g. description, vehicle reg etc.

Operation name or number

Date

Time of activity (from) (to)

Briefing location and time

Name of operator(s) relating to THIS log

Details of what was seen, to include ADVOKATE (as above).