The Regulation of Investigatory Powers Act Policy

June 2019

Date Last Reviewed:	May 2019
Approved by:	Audit & Standards Committee
Date Approved:	TO BE ADDED
Review Date:	June 2020
Document Owner:	Finance Director

Purpose

(For text in **bold**, see glossary of terms – Appendix 1)

The RIPA Policy covers the proper conduct of crime prevention activities that involve use of covert **directed surveillance, covert human intelligence sources** or the accessing of **communications data**. Application of the policy ensures that the Council is operating in accordance with the RIPA Act 2000 (the 2000 Act) as amended by the Protection of Freedoms Act 2012 (the 2012 Act). This policy sets out the Council's approach; it details the checks and balances in place to ensure that any use of covert techniques is lawful, necessary and proportionate.

Staff found to have breached the Acts or the Council's Code of Practice are deemed to have breached the Council's Employee Code of Conduct and will be liable to disciplinary action.

Related Documents

The Act must be considered in tandem with associated legislation including the Human Rights Act (HRA) as well as the General Data Protection Regulation **(**GDPR).

Investigations should be conducted in accordance with the Council's Counter Fraud Strategy & Counter Fraud Policy.

Who is Governed by this Policy

The RIPA Policy covers all council staff and those working on behalf of the Council who are engaged in prevention and detection activities which involve the use of surveillance, accessing communications data or use of covert human intelligence sources.

Executive Summary

Regulation of a Local Authority's use of surveillance, use of covert human intelligence sources and accessing of communications data is set out in the RIPA Act 2000 as amended by the Protection of Freedoms Act 2012

Local Authorities' abilities to use these investigation methods are restricted in nature and may only be used for the prevention and detection of serious crime or disorder. Local Authorities are not able to use **intrusive surveillance.** Powers relating to **directed surveillance** were amended by the Protection of Freedoms Act 2012 and the RIPA (Directed Surveillance and CHIS) (Amendment) Order 2012 to limit usage to the purpose of preventing or detecting a criminal offence where the potential punishment is a maximum term of at least 6 months of imprisonment or involving potential offences involving underage sales of tobacco and alcohol.

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. This order was updated by The Regulation of Investigatory Powers (Communications Data) Order 2010.

The Act also directs how applications will be made and how, and by whom, they may be approved, reviewed, renewed, cancelled and retained.

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 Human Rights Act. A public authority such as the Council can infringe those rights, if 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.

In line with the Code of Practice issued by Central Government associated with the 2012 Act, LBBD will only use covert surveillance under RIPA powers where it is proportionate and necessary to do so, and only in the investigation of serious criminal offences.

Contents

Page

Introduction

'It is essential that the Chief Executive, or Head of Paid Service, 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).

Directed Surveillance

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 means have been used or considered.

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) (Appendix 4) will be able to give advice and guidance on this legislation. The SRO will appoint a **RIPA Monitoring Officer** (RMO). The RMO will be responsible for the maintenance of a **central register** that will be available for inspection by the Investigatory Powers Commissioner's Office (IPCO). The format of the central register is set out in Appendix 6.

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. Best practice for compliance with evidential rules relating to photographs and video/CCTV footage is contained in Appendix 7. 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.

This policy does not affect the general usage of the council's CCTV system. However, if cameras are specifically targeted for 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 Head of Paid Service (or in his absence whoever deputises for them).

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 sufficient documented evidence that the alleged crime or disorder exists and when directed surveillance is a necessary and proportionate step to take to secure further evidence.

Low level surveillance, such as 'drive-bys' or everyday activity observed by officers during 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.

Necessary

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.

Proportionate

The authoriser must also believe the proposed activities 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.

Crime Threshold

The Regulation of Investigatory Powers (Directed Surveillance and CHIS) (Amendment) Order 2012 imposes a 'Crime Threshold' whereby only crimes which are either punishable by a maximum 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 under RIPA.

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 CD. The threshold came into effect on 1 November 2012.

A Local Authority **cannot** authorise directed surveillance for preventing disorder unless this involves a criminal offence(s) punishable (whether on summary conviction or indictment) by a maximum term of at least 6 months' imprisonment.

Thus, LBBD will 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.

LBBD will also continue to authorise the use of directed surveillance for 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 **may not authorise** the use of directed surveillance under RIPA to investigate disorder that does not involve criminal offences

An Authorising Officer's Aide-Memoire is provided at Appendix 8 to assist Authorising Officers when considering applications for directed surveillance.

Covert Human Intelligence Sources

A person who reports suspicion of an offence is not a **Covert Human Intelligence Source** (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 **covert relationship** with another person for covertly obtaining or disclosing information that they become a CHIS.

Any consideration on the use of CHIS can only be considered with prior discussion with the Chief Operating officer and/or Director of Law, Governance and Human Resources.

For some test purchases, it will be necessary to use a CHIS who is, or appears to be, under the age of 16 (a juvenile). Written parental consent for the use of a juvenile CHIS must be obtained prior to authorisation, and the duration of such an authorisation is 1 month instead of the usual 12 months. The Authorising Officer must be the Chief Executive or Deputy. **NOTE: A juvenile CHIS may not be used to obtain information about their parent or guardian.**

Officers considering the use of a CHIS under the age of 18, and those authorising such activity must be aware of the additional safeguards identified in The Regulation of Investigatory Powers (Juveniles) Order 2000 and its Code of Practice.

A vulnerable individual should only be authorised to act as a CHIS in the most exceptional circumstances. A vulnerable individual is a person who is, or may need, community care services by reason of mental or other disability, age or illness, and who may not be able to take care of themselves. The Authorising Officer in such cases must be the Chief Executive, who is the Head of Paid Service, or in their absence whoever deputises for them.

Any deployment of a CHIS should consider the safety and welfare of that CHIS. Before authorising the use or conduct of a CHIS, the authorising officer should ensure that an appropriate bespoke risk assessment is carried out to determine the risk to the CHIS of any assignment and the likely consequences should the role of the CHIS become known. This risk assessment must be specific to the case in question. The ongoing security and welfare of the CHIS, after the cancellation of the authorisation, should also be considered at the outset.

A CHIS handler is responsible for bringing to the attention of a CHIS controller any concerns about the personal circumstances of the CHIS, as far as they might affect the validity of the risk assessment, the conduct of the CHIS, and the safety and welfare of the CHIS.

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

1. 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

2. 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.

The Authorisation Process

The processes for applications and authorisations for directed surveillance and CHIS are similar, but note the differences set out in the CHIS section above. Directed Surveillance & CHIS applications are made using forms in Appendix 5.

The authorisation process involves the following steps:

Investigation Officer

1. 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.

2. A risk assessment must be conducted by the Investigation Officer within 7 days of the proposed start date. 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 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.

3. The Investigation Officer will pass the application through to one of their service's "gatekeepers" for review.

4. The gatekeeper, having reviewed the application, will forward the request to the RIPA Monitoring Officer or another officer within the Assurance Group. The application will be logged on the central register and assigned a unique reference number. The RIPA Monitoring Officer will then submit the application form to an authorising officer (see Appendix 4) for approval.

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)

6. The AO considers the application and if it is considered complete the application is signed off and returned to the Monitoring Officer who will log the outcome within the central register. This process, along with the initial application and dealings with the Monitoring Officer, can be completed through email.

7. An Authorising Officer's Aide-Memoire is provided at Appendix 8 to assist Authorising Officers when considering applications for directed surveillance.

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

9. Once final approval has been received the Investigation Officer will retain a copy and will create an appropriate diary method to ensure that any additional documents are submitted in good time.

Application to Magistrates Court

10. The countersigned application form will form the basis of the application to the Magistrates Court (see further below)

Authorised Activity

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

12. Where possible, private vehicles used for directed surveillance purposes should have keeper details blocked by the DVLA.

13. Consideration should be given to notifying the relevant police force intelligence units of the operation.

14. 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.

15. Evidential notes should be made by all officers engaged in the operation. These documents will be kept in accordance with the appropriate retention guidelines.

16. 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

17. As soon as the authorised activity has concluded the Investigation Officer will complete a Cancellation Form (Appendix 5).

18. Originals of the complete application, any review or renewal & the cancellation forms will be retained with the central register. Should the forms have been completed electronically, the Monitoring Officer will retain all correspondence.

Judiciary Authorisation

Under sections 37 and 38 of the Protection of Freedoms Act 2012 a local authority who wishes to authorise the use of directed surveillance or the use of a CHIS under RIPA will need to obtain an order approving the grant or renewal of an authorisation from a JP (a District Judge or lay magistrate) before it can take effect.

The acquisition of **Communications Data** (CD) by Local Authorities was also required but in June 2019 the process changed. The Home Office transitioned all public authorities from RIPA to IPA and this will impact on the communications data acquisition regime. The IPA introduced independent authorisation of CD requests

through the setting up of the Office for CD Authorisations (OCDA). From June 2019, all CD applications must be authorised by OCDA replacing the need to gain judicial approval.
If the JP is satisfied that the statutory tests have been met and that the use of the technique is necessary and proportionate, he/she will issue an order approving the grant or renewal for the use of the technique as described in the application.

The judicial approval mechanism is in addition to the existing authorisation process under the relevant parts of RIPA as outlined above. The current process of assessing the 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 LBBD will provide the JP with a copy of the original RIPA authorisation and the supporting documents setting out the case. This forms the basis of the application to the JP and should contain all information that is relied upon.

The original RIPA authorisation should be shown to the JP but also be retained by LBBD 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 take a copy.

Importantly, the appropriate officer will also need to provide the JP with a partially completed judicial application form.

Although the officer is required to provide a 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 JP and will be the official record of the JP's decision. The officer from LBBD will need to obtain judicial approval for all initial RIPA authorisations and renewals and will need to retain a copy of the judicial application form after it has been signed by the JP. There is no requirement for the JP to consider either cancellations or internal reviews.

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

It will be important for each officer seeking authorisation to establish contact with the HM Courts & Tribunals Service (HMCTS) administration at the magistrates' court. HMCTS administration will be the first point of contact for the officer when seeking a Judiciary approval. LBBD 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 JP 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 forms so that one can be retained by the JP. They should provide the court with a copy of the signed judicial application 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 JP 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 will be sworn in and present evidence or provide information as required by the JP. The hearing will be in private and heard by a single JP who will read and consider the RIPA authorisation and the judicial application form. He/she may have questions to clarify points or require additional reassurance on specific points.

The attending officer will need to be able to answer the JP's questions on the policy and practice of conducting covert operations and the detail of the case itself. 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 JP to make the case.

It is not LBBD's policy that legally trained personnel are required to make the case to the JP. 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 JP 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 has met the tests, then the JP 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 JP will record his/her decision on the order section of the judicial application form. HMCTS administration will retain a copy of the local authority RIPA authorisation and the judicial application form. This information will be retained securely. Magistrates' courts are not public authorities for the purposes of the Freedom of Information Act 2000.

LBBD will need to provide a copy of the order to the communications SPOC (Single Point of Contact) for all CD requests. SPOCs must not acquire the CD requested until the JP has signed the order approving the grant.

Authorisation periods

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

A written authorisation (unless renewed or cancelled) will cease to have effect after 3 months. 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 one month. Urgent oral authorisations or authorisations will unless renewed, cease to have effect after 72 hours.

Telecommunications Data - NAFN

The RIPA (Communications Data) Order 2003 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 presently the Operational Director, Enforcement Services Division and the Director of Public Health. NAFN will inform the Designated Person once the application is ready to be reviewed by the Designated Persons.

The relevant Designated Person will then access the restricted area of the NAFN website, using a special code, 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 Interception of Communications Commissioner Office.

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.

Handling of material and use of material as evidence

Material obtained from properly authorised directed surveillance or a CHIS may be used in other investigations. Arrangements in place for the handling, storage and destruction of material obtained using directed surveillance, a CHIS or the obtaining or disclosure of communications data 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.

Training

Officers conducting directed surveillance operations, using a CHIS or acquiring communications data along with Authorising Officers, the Senior Responsible Officer and the RIPA Monitoring Officer must be suitably qualified or trained.

The Senior Responsible Officer in conjunction with the RIPA Monitoring Officer is responsible for arranging suitable training for those conducting surveillance activity or using a CHIS.

All training will take place at reasonable intervals as determined by the Senior Responsible Officer, but it is envisaged that an update will usually be necessary following legislative or good practice developments.

Surveillance Equipment

All mobile surveillance equipment should be securely held and suitability for use discussed with the Security & Investigations or Assurance Group.

RIPA Record Quality Reviews

To ensure directed surveillance authorisations are being conducted in accordance with Council policy, a system of internal quality assurance has been put in place. The Audit & Select Committee will receive quarterly summaries on the Council's use of RIPA.

The Inspection Process

The Investigatory Powers Commissioner's Office (IPCO) will make periodic inspections during which the inspector will 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.

Resources

The latest Codes of Practice for RIPA can be found on the GOV.UK website at:

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

Further information can be found on the Investigatory Powers Commissioner's Office website & via the Home Office website:

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

http://www.homeoffice.gov.uk/counter-terrorism/regulation-investigatory-powers/

Relevant Acts:

Regulation of Investigatory Powers Act 2000:
http://www.legislation.gov.uk/ukpga/2000/23/contents

Protection of Freedoms Act 2012:
http://www.legislation.gov.uk/ukpga/2012/9/contents/enacted

Human Rights Act 1998:
http://www.legislation.gov.uk/ukpga/1998/42

General Data Protection Regulation:
https://www.eugdpr.org/eugdpr.org.html

The latest version of the RIPA Policy and our documents can be obtained either by contacting the Assurance Group directly or by visiting our intranet pages

If you have any comments or feedback to do with this document, we would like to hear from you, so please get in touch and email us at the following address:

caft@lbbd.gov.uk

Appendix 1 of F

GLOSSARY OF TERMS (For full definitions, refer to the Act)

Central Register
The primary record of RIPA & CHIS applications, reviews, renewals, and cancellations and where original documents are stored.

Collateral intrusion
The likelihood of obtaining private information about someone who is not the subject of the directed surveillance operation.

Communications Data
Information on the communication's origin, destination, route, time, date, size, duration, or type of underlying service but not the content.

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 Human Intelligence Source
A person who establishes or maintains a personal or other relationship for the covert purpose of using such a relationship to obtain information or to provide access to any information to another person or covertly discloses information

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.

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.

Monitoring Officer (MO)
The Monitoring Officer has the day to day responsibility to maintain a central and up-to-date record of all authorisations (Central Register) and arrange appropriate training.

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.

Reviewing Officer (RO)
The Head of Legal Services has been designated as the Reviewing Officer. The role is responsible for ensuring an oversight to the RIPA policy, an Authorising Officer as well as counter signatory in cases of non-RIPA applications.

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 of F

The Human Rights Act 1998

Key Articles of Schedule 1 of the Human Rights Act relevant to RIPA:

ARTICLE 6 RIGHT TO A FAIR TRIAL

1. In the determination of his civil rights and obligations or of any criminal charge against him, everyone is entitled to a fair and public hearing within a reasonable time by an independent and impartial tribunal established by law. Judgment shall be pronounced publicly but the press and public may be excluded from all or part of the trial in the interest of morals, public order or national security in a democratic society, where the interests of juveniles or the protection of the private life of the parties so require, or to the extent strictly necessary in the opinion of the court in special circumstances where publicity would prejudice the interests of justice.

2. Everyone charged with a criminal offence shall be presumed innocent until proved guilty according to law.

3. Everyone charged with a criminal offence has the following minimum rights:

   a. to be informed promptly, in a language which he understands and in detail, of the nature and cause of the accusation against him;
   b. to have adequate time and facilities for the preparation of his defence;
   c. to defend himself in person or through legal assistance of his own choosing or, if he has not sufficient means to pay for legal assistance, to be given it free when the interests of justice so require;
   d. to examine or have examined witnesses against him and to obtain the attendance and examination of witnesses on his behalf under the same conditions as witnesses against him;
   e. to have the free assistance of an interpreter if he cannot understand or speak the language used in court.

ARTICLE 8 RIGHT TO RESPECT FOR PRIVATE AND FAMILY LIFE

1. Everyone has the right to respect for his private and family life, his home and his correspondence.

2. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.

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

Appendix 3 of F

General Data Protection Regulations 2018

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-European Economic Area countries without adequate protection.

Under the GDPR, the data protection principles set out the main responsibilities for organisations. Article 5 of the GDPR requires that personal data shall be:

"a) processed lawfully, fairly and in a transparent manner in relation to individuals;

b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes;

c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;

d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;

e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals; and

f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures."

Article 5(2) requires that: "the controller shall be responsible for, and be able to demonstrate, compliance with the principles."

Key RIPA Officers

Authorisation of RIPA applications where there is a likelihood of obtaining Confidential Information can only be given by the Chief Executive or deputy.

Only the Chief Executive, as Head of Paid Service or their deputy, can authorise the use of a vulnerable person or a juvenile to be used as a Covert Human Intelligence Source.

Principal RIPA Officers

Claire Symonds Senior Responsible Officer (SRO)	Chief Operating Officer & Deputy Chief Executive
Kevin Key RIPA Monitoring Officer (MO)	Counter Fraud Manager: Assurance Group
Fiona Taylor Reviewing Officer (RO)	Director: Law & Governance

Authorising Officers

Chris Naylor	Chief Executive
Claire Symonds	Chief Operating Officer and SRO
Fiona Taylor	Director: Law, Governance & Human Resources and RO
Matthew Cole	Director of Public Health
Authorising Officer (AO)	Operational Director

Appointment of Staff designated as "Gatekeepers"

Name	**Designation**
Theo Lamptey	Service Manager, Public Protection
Simon Scott	Senior Investigator – Assurance Group
Jaiyesh Patel	Senior Investigator – Assurance Group

Appendix F

Appendix 5 of F

Judicial Oversight – LBBD Council's Authorised Applicants

I certify that the following have been appointed under Section 223(1) of the Local Government Act 1972 to appear for the Authority and are approved applicants in accordance with section 223(1) Local Government Act 1972:

List of all staff that have attended and passed the training

Name	**Section**	**Appointed from**
Glen Mark	Food Safety, Enforcement Service	12/12/2016
Meribel Mujih	Private Sector Housing, Regulatory Services	13/12/2016
Rob Harvey	Anti-Social Behaviour	13/12/2016
Nicholas Saunders	Anti-Social Behaviour	13/12/216
Pat Jarman	Assurance & Counter Fraud Group	25/01/2017
Arfan Naseem	CCTV & Security	25/01/2017
Geraldine Bowker	Anti-Social Behaviour	25/01/2017
Cenred Elworthy	Trading standards	25/01/2017
Carolyn Greenaway	Care Management	25/01/2017
Simon Scott	Assurance & Counter Fraud Group	26/01/2017
Vincent Searle	Trading Standards	26/01/2017
Natalie Males	Private Sector Housing, Enforcement Service	26/01/2017
Robert Redmond	Regulatory Services	26/01/2017

In addition; all Gatekeepers have attended training and are approved for the purpose of making applications.

Kevin Key
RIPA Monitoring Officer

Unique Reference Number	

RIPA Application Form

Part II of the Regulation of Investigatory Powers Act 2000

Application for Authorisation for Directed

Surveillance

Public Authority *(including full address)*			
Name of Applicant		**Unit/Branch /Division**	
Full Address			
Contact Details			
Investigation/Operation Name (if applicable)			
Investigating Officer (if a person other than the applicant)			

1. Give name and rank or position of authorising officer in accordance with the Regulation of Investigatory Powers (Directed Surveillance and Covert Human Intelligence Sources) Order 2010 No. 521. The exact position of the Authorising Officer should be given.
2. Describe the purpose of the specific operation or investigation.
3. Describe in detail the surveillance operation to be authorised and expected duration, including any premises, vehicles or equipment (e.g. camera, binoculars, recorder) that may be used.
4. The identities, where known, of those to be subject of the directed surveillance.
• **Name:** • **Address:** • **DOB:** • **Other information as appropriate:**
5. Explain the information that it is desired to obtain as a result of the directed surveillance.

6. Identify on which grounds the directed surveillance is <u>necessary</u> under Section 28(3) of RIPA. *Delete those that are inapplicable. Ensure that you know which of these grounds you are entitled to rely on (SI 2010 No.521).*
NB: UNDER SECTION 28 OF RIPA, THE ONLY GROUND AVAILABLE TO THE COUNCIL IS: "FOR THE PURPOSE OF PREVENTING OR DETECTING CRIME OR OF PREVENTING DISORDER". **THIS APPLICATION MUST BE REJECTED, IF THIS GROUND IS NOT RELEVANT TO THE PROPOSED SURVEILLANCE.**
7. Explain <u>why</u> this directed surveillance is necessary on the grounds you have identified [Code paragraph 3.3].
8. Supply details of any potential collateral intrusion and why the intrusion is unavoidable. [Bear in mind Code paragraphs 3.8 to 3.11.] **Describe precautions you will take to minimise collateral intrusion.**
9. Explain <u>why</u> this directed surveillance is proportionate to what it seeks to achieve. How intrusive might it be on the subject of surveillance or on others? And why is this intrusion outweighed by the need for surveillance in operational terms or can the evidence be obtained by any other means [Code paragraphs 3.4 to 3.7]?

10. Confidential information [Code paragraphs 4.1 to 4.31]. INDICATE THE LIKELIHOOD OF ACQUIRING ANY CONFIDENTIAL INFORMATION:

11. Applicant's Details			
Name (print)		**Tel No:**	
Grade and Rank or position		**Date**	
Signature			

12. Authorising Officer's Statement. [Spell out the "5 Ws" – Who; What; Where; When; Why and HOW– in this and the following box.]
I hereby authorise directed surveillance defined as follows: [*Why is the surveillance necessary, Whom is the surveillance directed against, Where and When will it take place, What surveillance activity/equipment is sanctioned, How is it to be achieved?]*

13. Explain <u>why</u> you believe the directed surveillance is necessary [Code paragraph 3.3]. **Explain <u>why</u> you believe the directed surveillance to be proportionate to what is sought to be achieved by carrying it out [Code paragraphs 3.4 to 3.7].**

14. (Confidential Information Authorisation.) Supply detail demonstrating compliance with Code paragraphs 4.1 to 4.31.				
Date of first review				
Programme for subsequent reviews of this authorisation: [Code paragraph 3.23]. Only complete this box if review dates after first review are known. If not or inappropriate to set additional review dates then leave blank.				
Name (Print)		**Grade and Rank/Position**		
Signature		**Date and time**		
Expiry date and time [e.g.: authorisation granted on 1 April 20016 - expires on 30 June 2016, 23:59]				

15. Urgent Authorisation [Code paragraph 5.9]: Authorising officer: explain why you considered the case so urgent that an oral instead of a written authorisation was given.				
16. If you are only entitled to act in urgent cases: explain why it was not reasonably practicable for the application to be considered by a fully qualified authorising officer.				
Name (Print)		**Grade and Rank or position**		
Signature		**Date and Time**		
Urgent authorisation Expiry date:		**Expiry time:**		
Remember the 72-hour rule for urgent authorities – check Code of Practice.		e.g. authorisation granted at 5pm on June 1st expires 4.59pm on 4th June		

Unique Reference Number	

RIPA Renewal Form

Part II of the Regulation of Investigatory Powers Act 2000

Renewal of a Directed Surveillance Authorisation

Public Authority *(including full address)*	

Name of Applicant		**Unit/Branch /Division**	
Full Address			
Contact Details			
Investigation/Operation Name (if applicable)			
Renewal Number			

Details of renewal:

1. Renewal numbers and dates of any previous renewals.	
Renewal Number	**Date**

2. Detail any significant changes to the information as listed in the original authorisation as it applies at the time of the renewal.

3. Detail the reasons why it is necessary to continue with the directed surveillance.

4. Detail why the directed surveillance is still proportionate to what it seeks to achieve.

5. Indicate the content and value to the investigation or operation of the information so far obtained by the directed surveillance.

6. Give details of the results of the regular reviews of the investigation or operation.

7. Applicant's Details			
Name (Print)		**Tel No**	
Grade/Rank		**Date**	
Signature			

8. Authorising Officer's Comments. <u>This box must be completed.</u>

9. Authorising Officer's Statement.			
I, [insert name], hereby authorise the renewal of the directed surveillance operation as detailed above. The renewal of this authorisation will last for 3 months unless renewed in writing. This authorisation will be reviewed frequently to assess the need for the authorisation to continue.			
Name (Print)	----------	**Grade / Rank**	----------
Signature	----------	**Date**	----------
Renewal From:	**Time:**	**Date:**	

Date of first review.	
Date of subsequent reviews of this authorisation.	

Unique Reference Number	

RIPA Review Form

Part II of the Regulation of Investigatory Powers Act 2000

Review of a Directed Surveillance authorisation

Public Authority *(including address)*			
Applicant		**Unit/Branch /Division**	
Full Address			
Contact Details			
Operation Name		**Operation Number*** *Filing Ref	
Date of authorisation or last renewal		**Expiry date of authorisation or last renewal**	
		Review Number	

Details of review:

1. Review number and dates of any previous reviews.	
Review Number	

2. Summary of the investigation/operation to date, including what private information has been obtained and the value of the information so far obtained.
3. Detail the reasons why it is necessary to continue with the directed surveillance.
4. Explain how the proposed activity is still proportionate to what it seeks to achieve.
5. Detail any incidents of collateral intrusion and the likelihood of any further incidents of collateral intrusions occurring.
6. Give details of any confidential information acquired or accessed and the likelihood of acquiring confidential information.

7. Applicant's Details

Name (Print)		**Tel No**	
Grade/Rank		**Date**	
Signature			

8. Review Officer's Comments, including whether or not the directed surveillance should continue.

9. Authorising Officer's Statement.			
I, [insert name], hereby agree that the directed surveillance investigation/operation as detailed above [should/should not] continue [until its next review/renewal] [it should be cancelled immediately].			
Name (Print):	----------	**Grade / Rank**	----------
Signature:	----------	**Date:**	----------

10. Date of next review	

Unique Reference Number	

RIPA Cancellation Form

Part II of the Regulation of Investigatory Powers Act 2000

Cancellation of a Directed Surveillance authorisation

Public Authority *(including full address)*	

Name of Applicant		**Unit/Branch/Division**	
Full Address			
Contact Details			
Investigation/Operation Name (if applicable)			

Details of cancellation:

1. Explain the reason(s) for the cancellation of the authorisation:

2. Explain the value of surveillance in the operation:

3. Authorising officer's statement.			
I, [**insert name**], hereby authorise the cancellation of the directed surveillance investigation/operation as detailed above.			
Name (Print)	_____	**Grade**	.....
Signature	_____	**Date**	.....

4. Time and Date of when the authorising officer instructed the surveillance to cease.			
Date:		**Time:**	

5. Authorisation cancelled.	**Date:**	**Time:**

Forms can also be obtained from the Assurance and Counter Fraud Group at: caft@lbbd.gov.uk

Or can be printed of and completed as required from the GOV.UK website at:

RIPA Application for Directed Surveillance

Renewal of a Directed Surveillance Authorisation

Review of a Directed Surveillance Authorisation

Cancellation of a Directed Surveillance Authorisation

Appendix F

Appendix 7 of F

Central Register

A central register will be maintained by the RIPA Monitoring Officer. The register will contain details of all RIPA and CHIS applications (whether approved or not) and all reviews, renewals and cancellations.

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

The register will also contain the following information:

- 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 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 will be available for inspection by the Office of the Surveillance Commissioners.

The register will form the basis of statistical returns of RIPA usage by the Council which are periodically compiled.

Best practice regarding photographic and video evidence

Photographic or video evidence can be used to support the verbal evidence of what the officer conducting surveillance actually saw. There will also be occasions when video footage may be obtained without an officer being present at the scene. However, it is obtained, it must be properly documented and retained in order to ensure evidential continuity. All such material will be disclosable in the event that a prosecution ensues.

Considerations should be given as to how the evidence will eventually be produced. This may require photographs to be developed by an outside laboratory. Arrangements should be made in advance to ensure continuity of evidence at all stages of its production. A new film, tape or memory card should be used for each operation.
If video footage is to be used, start it with a verbal introduction to include day, date, time and place and names of officer's present. Try to include footage of the location, e.g. street name or other landmark so as to place the subject of the surveillance.

A record should be maintained to include the following points:

- Details of the equipment used
- Name of the officer who inserted the film, tape or memory card into the camera
- Details of anyone else to whom the camera may have been passed
- Name of officer removing film, tape or memory card
- Statement to cover the collection, storage and movement of the film, tape or memory card
- Statement from the person who developed or created the material to be used as evidence

As soon as possible the original recording should be copied, and the master retained securely as an exhibit. If the master is a tape, the record protect tab should be removed once the tape has been copied. Do not edit anything from the master. If using tapes, only copy on a machine that is known to be working properly. Failure to do so may result in damage to the master.

Stills may be taken from video. They are a useful addition to the video evidence.

Checklist 6: Compiling an Audit Trail for Digital Images
in the National Policing Improvement Agency's document:
"PRACTICE ADVICE ON POLICE USE OF DIGITAL IMAGES which is available at:

http://library.college.police.uk/docs/acpo/police-use-of-digital-images-2007.pdf

provides a list of what information should be included (with date and time of action) in order to make the evidence admissible.

Appendix F

Appendix 9 of F

Authorising Officer's Aide-Memoire

Has the applicant satisfactorily demonstrated proportionality? Court will ask itself should (not could) we have decided this was proportionate. Is there a less intrusive means of obtaining the **same** information? What is the risk – to the authority (loss), to the community of allowing the offence to go un-investigated? What is the potential risk to the subject? What is the least intrusive way of conducting the surveillance? Has the applicant asked for too much? Can it safely be limited? Remember – Don't use a sledge-hammer to crack a nut! YOUR COMMENTS	**Yes**	**No**

Has the applicant satisfactorily demonstrated necessity? What crime is alleged to be being committed? Has the applicant described it in full? Is surveillance necessary for what we are seeking to achieve? Does the activity need to be covert, or could the objectives be achieved overtly? YOUR COMMENTS	**Yes**	**No**

What evidence does applicant expect to gather? Has applicant described: (a) what evidence he/she hopes to gain, and (b) the value of that evidence in relation to THIS enquiry? YOUR COMMENTS	**Yes**	**No**
Is there any likelihood of obtaining confidential information during	**Yes**	**No**

this operation? **If "Yes" operation must be authorised by the Chief Executive or in their absence their deputy.**		

Have any necessary risk assessments been conducted before requesting authorisation? Detail what assessment (if any) was needed in this particular case. In the case of a CHIS authorization an appropriate bespoke risk assessment must be completed.	**Yes**	**No**

When applying for **CHIS** authorisation, have officers been identified to: a) have day to day responsibility for the CHIS (a handler) b) have general oversight of the use of the CHIS (a controller) c) be responsible for retaining relevant CHIS records, including true identity, and the use made of the CHIS.	**Yes**	**No**

Have all conditions necessary for authorisation been met to your satisfaction? GIVE DETAILS	**Yes**	**No**

Do you consider that it is necessary to place limits on the operation? IF YES, GIVE DETAILS (e.g. no. of officers, time, date etc.) and REASONS	**Yes**	**No**

Remember to diarise any review dates and any subsequent action necessary by you and/or applicant. Return copy of completed application to applicant and submit original to the Assurance and Counter Fraud Group. Retain copy.

Open Source

Investigators make much use of the internet to assist with their enquiries. Many of the checks completed could be considered 'open source' that are unlikely to amount to either Directed Surveillance or the use of a CHIS. However, consideration must be had for certain circumstances where RIPA authorisation may be deemed appropriate.

a. Normal Use

When an investigator makes normal checks on the internet, accessing information held within the public domain, on a single occasion, this would be considered acceptable and within the bounds of normal usage. Full records must be kept taking into consideration the expectations of the Criminal Procedure and Investigations Act. Throughout an investigation, it would be appropriate for an investigator to make ***occasional*** further checks. If, on the other hand, it becomes apparent that regular checks are taking place to monitor someone's activities, this may constitute Directed Surveillance.

b. Directed Surveillance

When regular checks of the same pages occur, in order to monitor activity, this may be Directed Surveillance. Should this be happening, consideration should be had for the use of RIPA.

c. Covert Human Intelligence Source

Looking at publicly available pages is considered 'Open Source' but should a decision be made to request access to view page then the situation changes. In order to access specific information a personal or other relationship would have to be created or maintained potentially amounting to the use of a CHIS. An example where this is likely is sending a friend request within Facebook.

EXCEPTION

Should you use an identity that is overt (such as LBBD Fraud Investigations or LBBD trading Standards) to send the request from. In this instance, it would be classed as monitoring and not Directed Surveillance/CHIS.

Officers are encouraged to follow the procedures of this policy (either RIPA or Non-RIPA) should the above circumstances present themselves.

Flow Chart for RIPA Applications