Values and Ethics Sub-Committee

Agenda

Date: Monday, 28 September 2020
Time: 1.00 pm
Venue: Remote Access - Remote Access

Distribution:

Councillors: Adebola Adebayo, Mark Brain, Tim Kent, Liz Radford and Clive Stevens

Copies to: Nancy Rollason (Head of Legal Service), Allison Taylor (Democratic Services Officer), Lucy Fleming (Head of Democratic Engagement) and Louise deCordova (Democratic Services Manager)

Issued by: Allison Taylor, Democratic Services
City Hall, PO Box 3176, Bristol, BS3 9FS
Tel: 0117 92 22237
E-mail: democratic.services@bristol.gov.uk
Date: Friday, 18 September 2020

Agenda

1. Welcome, Introductions and Apologies for Absence.

2. Declarations of Interest

3. Minutes of previous meeting.

Report to follow.

4. Regulation of Investigatory Powers Act 2000 (RIPA)

(Pages 3 - 30)

Public Information Sheet

Inspection of Papers - Local Government (Access to Information) Act 1985

You can find papers for all our meetings on our website at https://www.bristol.gov.uk/council-meetings

Covid-19: changes to how we hold public meetings

Following changes to government rules, we'll use video conferencing to hold all public meetings, including Cabinet, Full Council, regulatory meetings (where planning and licensing decisions are made) and scrutiny.

Councillors will use Zoom or Skype for Business to take part in the meetings and vote on agenda items.

We'll stream the meetings live on YouTube.

You can submit statements, questions and petitions ahead of the meetings in the same way as usual. We will send all statements to participating Councillors in advance and respond to all questions and petitions in writing.

You will not be able to present a public submission at the meeting at the current time. We're looking into options for increasing public participation at meetings held using video conferencing, including being able to present a statement or ask supplementary questions using Zoom. We hope to have this in place in by late May 2020.

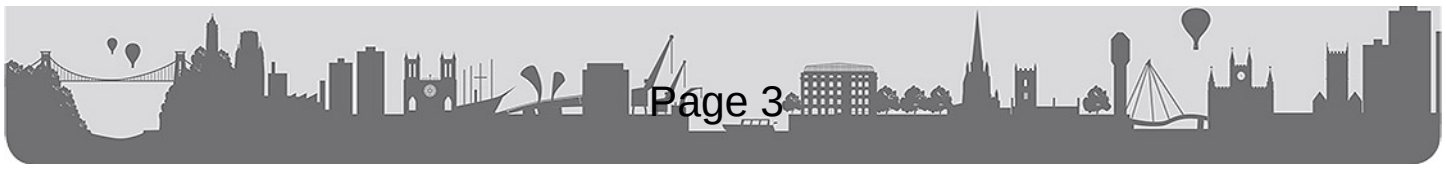
Email democratic.services@bristol.gov.uk if you have any questions.

Public Forum

Members of the public may make a written statement ask a question or present a petition to most meetings. Your statement or question will be sent to the Committee. Please submit it to democratic.services@bristol.gov.uk The following requirements apply:

- The statement is received no later than **12.00 noon on the working day before the meeting** and is about a matter which is the responsibility of the committee concerned.
- The question is received no later than **5pm three clear working days before the meeting**.
- Any statement submitted should be no longer than one side of A4 paper. For copyright reasons, we are unable to reproduce or publish newspaper or magazine articles that may be attached to statements.

By participating in public forum business, we will assume that you have consented to your name and the details of your submission being recorded and circulated to the Committee and published within the minutes. Your statement or question will also be made available to the public at the meeting to which it relates and may be provided upon request in response to Freedom of Information Act requests in the future.



We will try to remove personal and identifiable information. However, because of time constraints we cannot guarantee this, and you may therefore wish to consider if your statement contains information that you would prefer not to be in the public domain. Public Forum statements will not be posted on the council's website. Other committee papers may be placed on the council's website and information within them may be searchable on the internet.

During the meeting:

- Public Forum is normally one of the first items on the agenda, although statements and petitions that relate to specific items on the agenda may be taken just before the item concerned.
- There will be no debate on statements or petitions. Public Forum will be circulated to the Committee members prior to the meeting and then noted at the meeting.
- Please note that only written submissions can be considered at this time.

For further information about procedure rules please refer to our Constitution
https://www.bristol.gov.uk/how-council-decisions-are-made/constitution

The privacy notice for Democratic Services can be viewed at www.bristol.gov.uk/about-our-website/privacy-and-processing-notices-for-resource-services

Webcasting/ Recording of meetings

Members of the public attending meetings or taking part in Public forum are advised that all Full Council and Cabinet meetings and some other committee meetings are now filmed for live or subsequent broadcast via the council's webcasting pages. The whole of the meeting is filmed (except where there are confidential or exempt items).

Other formats and languages and assistance for those with hearing impairment

You can get committee papers in other formats (e.g. large print, audio tape, braille etc) or in community languages by contacting the Democratic Services Officer. Please give as much notice as possible. We cannot guarantee re-formatting or translation of papers before the date of a particular meeting.

Values and Ethics Sub Committee

28 September 2020

Report of: Director: Legal & Democratic Services

Title: Regulation of Investigatory Powers Act 2000 (RIPA)

Ward: Citywide

Officer presenting report: Director: Legal & Democratic Services

Recommendation
To note the report on the Council's use of the powers available to it under the Regulation of Investigatory Powers Act 2000 and the report of the Investigatory Powers Commissioner's inspection.

Summary
The Terms of Reference of the Values and Ethics sub-committee require the sub-committee to review the Council's use of the powers available to it under the Regulation of Investigatory Powers Act 2000'RIPA'. RIPA sets out a regulatory framework for the use of covert investigatory techniques by public authorities. The Investigatory Powers Commissioner's Office 'IPCO' regulates RIPA and carries out regular inspections. The Council was the subject of an inspection in June 2020.

Policy

1. The Council's Regulation of Investigatory Powers Act 2000 Policy and Procedure is attached as Appendix A. This document sets out the policy and procedures adopted by Bristol City Council in relation to RIPA.

Consultation

Internal

2. Not applicable

External

3. Not applicable.

Context

4. RIPA sets out a regulatory framework for the use of covert investigatory techniques by public authorities that is likely to result in the obtaining of private information about a person. This includes directed surveillance, interceptions of private communications (eg phone calls and emails), and use of covert human intelligence sources.

5. RIPA does not include any specific provisions to empower Council officers to carry out covert activities. Rather, if such activities are conducted by council officers, then RIPA regulates them in a manner to ensure that the activity is compatible with the European Convention on Human Rights (ECHR), particularly Article 8 - the right to respect for private and family life.

6. RIPA requires any covert surveillance to be authorised in advance by a designated authorising officer and by the Magistrates' Court. Local authorities can only apply for RIPA authorisations to carry out covert surveillance for preventing or detecting a criminal offence which would be punishable by a prison sentence of at least six months or for age related sale of alcohol and tobacco or nicotine inhaling products.

7. Before applying for an authorisation under RIPA, officers need to consider the use of less intrusive methods. The authorisation lasts for a specified period and must be regularly reviewed and cancelled when no longer required. All RIPA applications, authorisations, reviews, renewals and cancellations are retained in one central record with auditable, unique reference numbers to be retained for five years. The central record is held by Legal Services.

8. In 2019/2020 Bristol City Council carried out surveillance authorised under RIPA twice. Details are set out in the 2019 RIPA Register in exempt Appendix B

9. The Council must appoint a Senior Responsible Officer for RIPA. This role is carried out by the Director: Legal and Democratic Services who has regular meetings with the RIPA Monitoring Officer to inspect the RIPA register and to maintain oversight of the use of the Council's RIPA powers. A RIPA training webinar together with template forms and guidance is available for all officers on the Source. In September 2019 external training was commissioned for all officers who might carry out surveillance including child protection and adult social workers as well as enforcement officers from Regulatory Services. Training will be arranged again in 2021.

10. On 4th June the IPCO inspector considered the RIPA central record and conducted a video interview with Senior Responsible Officer for RIPA and the RIPA Monitoring Officer. The inspector's report and measures taken thereafter to comply with the recommendations are detailed in exempt Appendix C. The information provided demonstrated a level of compliance that removed the requirement for a physical inspection.

Other Options Considered

11. None necessary.

Risk Assessment

12. Not applicable.

Legal and Resource Implications

Legal implications:

13. As above.

Financial:

14. Not applicable

Land/Property:

15. Not applicable.

Human Resources:

16. Not applicable.

Appendices:

Appendix A – Regulation of Investigatory Powers Act 2000 Policy and Procedure
Appendix B - EXEMPT
Appendix C - EXEMPT

LOCAL GOVERNMENT (ACCESS TO INFORMATION) ACT 1985
Background Papers: None

BRISTOL CITY COUNCIL

Regulation of Investigatory Powers Act 2000

Policy and Procedure

BRISTOL CITY COUNCIL
LEGAL SERVICES
September 2019

Bristol City Council Policy Statement Regulation of Investigatory Powers Act 2000

Contents

1 INTRODUCTION

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

1.2 The following terms are used throughout this Policy:

RIPA -Regulation of Investigatory Powers Act 2000

CHIS -Covert Human Intelligence Source

SPoC -Single Point of Contact

SRO-Senior Responsible Officer

IPCO -Investigatory Powers Commissioner's Office

NAFN -National Anti-Fraud Network

CSP-Communications Service Provider

1.3 RIPA sets out a regulatory framework for the use of covert investigatory techniques by public authorities. RIPA does not provide any powers to carry out covert activities. If such activities are conducted by council officers, then RIPA regulates them in a manner that is compatible with the European Convention on Human Rights (ECHR), particularly Article 8, the right to respect for private and family life. It should be noted that any use of activities under RIPA will be as a last resort and council policy is not to undertake such activities unless absolutely necessary.

1.4 Further information on RIPA, including guidance on completion of forms and a summary of terms can be found on the Source

2 PURPOSE AND OBJECTIVES

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

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

3 ROLES AND RESPONSIBILITIES

3.1 Senior Responsible Officer (SRO):

3.1.1 The role of SRO will be undertaken by the council's Head of Legal and Democratic Services.

3.1.2 The SRO will be responsible for:

• The integrity of the process in place within the council for the management of CHIS and Directed Surveillance;

• Ensuring that all authorising officers are of an appropriate standard;

• Compliance with Part 2 of the Act and with the Home Office Codes of Practice;

• Oversight of the reporting of errors to the relevant Commissioner and the identification of both the cause(s) of errors and the implementation of processes to minimise repetition of errors;

• Engagement with the Investigatory Powers Commissioner's Office (IPCO) inspectors when they conduct their inspections, where applicable; and

• Where necessary, oversight of the implementation of post-inspection action plans approved by the relevant oversight Commissioner.

3.2 Authorising Officers

3.2.1 The officers named in Appendix A shall be the only officers within the council who can authorise applications under RIPA in accordance with the procedures set out in section 7 of this policy.

3.3 Each of the Authorising Officers can authorise applications, for onward consideration by a Magistrate. Each Authorising Officer may authorise renewals and cancellations, and undertake reviews, in relation to any investigation carried out, or proposed to be carried out, by officers. Authorising Officers may not sub-delegate their powers in relation to RIPA to other officers.

3.4 The officer who authorises a RIPA application should also carry out the review, renewal and cancellation. The Cancellation form must contain sufficient detail as to the type and nature of surveillance undertaken as well as how it assisted the

investigation. Further, the Authorising Officer must outline and explain on the cancellation form how the product of the surveillance (if any) is to be managed. If the original Authorising Officer is not available to undertake the review, renewal or cancellation, this can be undertaken by any other Authorising Officer.

3.5 RIPA Monitoring Officer:

3.5.1 The lawyer named in Appendix A has been appointed RIPA Monitoring Officer.

3.5.2 The RIPA Monitoring Officer shall:-

• have overall responsibility for the management and oversight of requests and authorisations under RIPA;

3.6 RIPA Administrator

3.6.1 The RIPA Administrator is the Legal Officer named in Appendix A

3.6.2 The RIPA administrator shall

• issue a unique reference number to each authorisation requested under RIPA

• retain a copy of the application and authorisation together with any supplementary documentation and notification of the approval given by the authorising officer maintain a central RIPA records file matrix entering the required information as soon as the forms/documents are received in accordance with the relevant Home Office Code of Practice;

• review and monitor all forms and documents received to ensure compliance with the relevant law and guidance and this policy and procedures document in consultation with the RIPA Monitoring Officer and inform the Authorising Officer of any concerns;

• chase failures to submit documents and/or carry out reviews/cancellations;

3.7 Councillors:

3.7.1 The Audit Committee for Bristol City Council will review the Council's use of RIPA on a periodic basis.

4 LOCAL AUTHORITY USE OF RIPA

4.1 RIPA limits local authorities to using three covert techniques – these are: Directed Surveillance, a Covert Human Intelligence Source (CHIS) and Communications Data. These three permitted uses of covert techniques are explained below. **The Local Authority is prohibited by law from conducting Intrusive Surveillance.**

• Directed surveillance

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

- Communications data

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

4.3 Officers should be aware of the scope and extent of activities covered by the provisions of RIPA. In many cases investigations carried out by council officers will not be subject to RIPA, as they involve overt rather than covert surveillance

5. DIRECTED SURVEILLANCE

Directed surveillance may only be authorised by the Council under RIPA for the purpose of preventing or detecting criminal offences that are either punishable, whether on summary conviction or indictment, by a maximum term of at least 6 months' imprisonment or are related to the underage sale of alcohol and tobacco

An explanation of terms used is set out below:

5.1. 'Surveillance' for the purposes of the Act includes

• monitoring, observing, listening to persons, watching or following their movements, listening to their conversations and other such activities or communications;

• recording anything mentioned above in the course of authorised surveillance;

• surveillance by, or with the assistance of, appropriate surveillance device(s).

Surveillance can be overt or covert.

5.2. Covert Surveillance

Covert Surveillance is surveillance carried out in a manner calculated to ensure that the person subject to the surveillance is unaware that it is, or may be taking place.

5.3 Directed Surveillance

Directed Surveillance is surveillance which:-

• is covert; and

• is not intrusive surveillance (see definition below - the council is prohibited by law from carrying out any intrusive surveillance);

• is not carried out as an immediate response to events where it would not be practicable to obtain authorisation under the Act;

• is likely to result in the obtaining of private information about a person (whether or not one specifically identified for the purposes of the investigation or operation).

5.4 Private information

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

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

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

5.5 Overt Surveillance

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

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

5.5.3 Similarly, surveillance will be overt if the subject has been told it will happen. This will be the case where a noisemaker is warned that recordings will be made if the noise continues; or where an entertainment licence is issued subject to conditions, and the licensee is told that officers may visit without notice or without identifying themselves to the owner/proprietor to check that the conditions are being met. Such warnings should be given to the person concerned in writing.

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

5.5.5 .Although signposted CCTV cameras do not normally require authorisation, this will be required if the camera(s) are to be directed for a specific purpose which involves surveillance on a particular person. (See Section 12 for guidance on the authorisation of directed surveillance undertaken by means of the council's CCTV cameras.)

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

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

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

5.8 Intrusive Surveillance

5.8.1 Intrusive Surveillance occurs when surveillance:

• is covert;

• relates to residential premises and/or private vehicles; and

• involves the presence of a person in the premises or in the vehicle or is carried out by a surveillance device in the premises/vehicle. Surveillance equipment mounted

outside the premises will not be intrusive, unless the device consistently provides information of the same quality and detail as might be expected if they were in the premises/vehicle.

5.9 Social Networking Sites (SNS) The Home Office Revised Code of Practice on Covert Surveillance and Property Interference, published in August 2018, provides the following guidance in relation to online covert activity:

'The growth of the internet, and the extent of the information that is now available online, presents new opportunities for public authorities to view or gather information which may assist them in preventing or detecting crime or carrying out other statutory functions, as well as in understanding and engaging with the public they serve. It is important that public authorities are able to make full and lawful use of this information for their statutory purposes. Much of it can be accessed without the need for RIPA authorisation; use of the internet prior to an investigation should not normally engage privacy considerations. But if the study of an individual's online presence becomes persistent, or where material obtained from any check is to be extracted and recorded and may engage privacy considerations, RIPA authorisations may need to be considered. The following guidance is intended to assist public authorities in identifying when such authorisations may be appropriate.

5.9.1 The internet may be used for intelligence gathering and/or as a surveillance tool. Where online monitoring or investigation is conducted covertly for the purpose of a specific investigation or operation and is likely to result in the obtaining of private information about a person or group, an authorisation for directed surveillance should be considered, as set out elsewhere in this code. Where a person acting on behalf of a public authority is intending to engage with others online without disclosing his or her identity, a CHIS authorisation may be needed (paragraphs 4.10 to 4.16 of the Covert Human Intelligence Sources code of practice provide detail on where a CHIS authorisation may be available for online activity).

5.9.2 In deciding whether online surveillance should be regarded as covert, consideration should be given to the likelihood of the subject(s) knowing that the surveillance is or may be taking place. Use of the internet itself may be considered as adopting a surveillance technique calculated to ensure that the subject is unaware of it, even if no further steps are taken to conceal the activity. Conversely, where a public authority has taken reasonable steps to inform the public or particular individuals that the surveillance is or may be taking place, the activity may be regarded as overt and a directed surveillance authorisation will not normally be available.

5.9.3 As set out below, depending on the nature of the online platform, there may be a reduced expectation of privacy where information relating to a person or group of people is made openly available within the public domain, however in some circumstances privacy implications still apply. This is because the intention when

making such information available was not for it to be used for a covert purpose such as investigative activity. This is regardless of whether a user of a website or social media platform has sought to protect such information by restricting its access by activating privacy settings.

5.9.4 Where information about an individual is placed on a publicly accessible database, for example the telephone directory or Companies House, which is commonly used and known to be accessible to all, they are unlikely to have any reasonable expectation of privacy over the monitoring by public authorities of that information. Individuals who post information on social media networks and other websites whose purpose is to communicate messages to a wide audience are also less likely to hold a reasonable expectation of privacy in relation to that information.

5.9.5 Whether a public authority interferes with a person's private life includes a consideration of the nature of the public authority's activity in relation to that information. Simple reconnaissance of such sites (i.e. preliminary examination with a view to establishing whether the site or its contents are of interest) is unlikely to interfere with a person's reasonably held expectation of privacy and therefore is not likely to require a directed surveillance authorisation. But where a public authority is systematically collecting and recording information about a particular person or group, a directed surveillance authorisation should be considered. These considerations apply regardless of when the information was shared online.

6. COMMUNICATIONS DATA

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

o 'Traffic data' (which includes information about where the communications are made or received) is classed as an intrusive type of data.

o 'service use information' (such as the type of communication, time sent and its duration); and

o 'subscriber information' (which includes billing information such as the name, address and bank details of the subscriber of telephone or internet services) the second and third examples are not classed as intrusive types of communications data.

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

6.3. The Investigatory Powers Act 2016 (IPA) is now the main legislation governing communications data. This includes the Acquisition of Communications data by local authorities and wider public authorities. It brings the relevant powers together but does not fully replace pre-existing legislation - so care will need to be taken to

ensure the correct legislative basis is used for operations, as the Investigatory Powers Act affects the way investigations are conducted.

Officers involved with the acquisition of communication data will need to comply with the provisions set out in the Investigatory Powers Act. It should you the first point of reference for officers carrying out work of this nature.

6.4 Under RIPA/IPA a local authority can obtain the less intrusive types of communications data: service use and subscriber information through The National Anti-Fraud Network (NAFN - see below). The introduction of the IPA enables local authorities to obtain more intrusive types of communication data (sometimes called 'traffic'). There is however, a serious crime threshold test (set out below) as well as an approval procedure to be followed through the Office for Communications Data Authorisations.

6.5 Council's Authorising Officers may not authorise the acquisition of communications data **unless** it is for the purpose of preventing or detecting a criminal offence and it meets certain conditions. This is known as the 'serious crime test'

What counts as a Serious Crime?

- An offence that is capable of attracting a prison sentence of 12 months or more
- An offence by a person who is not an individual (i.e. a corporate body)
- An offence falling within the definition of serious crime in section 81(3)(b) of the Act

(i.e. where the conduct involves the use of violence, results in substantial financial gain or is by a large number of person in pursuit of a common purpose)

- An offence which involves, as an integral part of it, the sending of a communication
- An offence which involves, as an integral part of it, a breach of a person's privacy

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

6.7 The National Anti-Fraud Network (NAFN) provides a SPoC service to local authorities and thus must be used in relation to all applications.

7 COVERT HUMAN INTELLIGENCE SOURCE

7.1 A CHIS is defined as the use of an individual to create a relationship with a subject, for the purposes of obtaining information, where the purpose of the relationship is not disclosed to the subject. Interaction with the subject of surveillance is therefore required in order for an individual to be regarded as a covert human intelligence source (CHIS). Activities of an undercover officer could fall within this definition. Additional careful monitoring and recording is required (see Home Office Code of Practice CHIS chapter 6).

7.2 The use of a covert human intelligence source (CHIS), and his or her conduct, also requires authorisation under RIPA. It is considered unlikely that there will be any circumstances which would require the council to either use a CHIS or operate under cover and advice should be sought from the Senior Responsible Officer before any authorisation is applied for or granted. hese provisions would cover the use of professional witnesses to obtain evidence or information, or officers operating "undercover". Great caution should be exercised in these circumstances.

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

• where members of the public volunteer information to the council as part of their normal civic duties;

• where the public contact telephone numbers set up by the council to receive information;

• where members of the public are asked to keep diaries of incidents in relation to, for example, planning enforcement, anti-social behaviour or noise nuisance. However, in certain circumstances, RIPA authorisation may be required if the criteria in section 26(2) of the Act are met.

8 AUTHORISATION PROCEDURES

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

8.2 The acquisition of communications data can only be undertaken by a SPoC (although the same authorisation procedures will apply). If necessary the council would engage a third party to undertake this role.

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

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

8.5 Authorisations will not take effect until a Magistrate has made an order approving the grant of the authorisation. It is vital that any surveillance for which authorisation has been sought does not start until such time as it has been approved by a Magistrate

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

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

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

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

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

8.11 When considering an application, Authorising Officers must:

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

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

(i) in accordance with the law;

(ii) necessary in the circumstances of the particular case; and

(iii) proportionate to what it seeks to achieve.

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

• The custodial sentence applicable to the offence being investigated;

• Balancing the size and scope of the proposed activity against the gravity and extent of the perceived crime or offence;

• Explaining how and why the methods to be adopted will cause the least possible intrusion on the subject and others;

• Whether the activity is an appropriate use of the legislation and a reasonable way, having considered all practical alternatives, of obtaining the necessary result;

• Evidencing, as far as reasonably practicable, what other methods had been considered and why they were not implemented.

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

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

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

(a) be satisfied that the conduct and/or use of the CHIS is proportionate to the objective sought to be achieved;

(b) be satisfied that appropriate arrangements are in place for the management and oversight of the CHIS. These arrangements must address health and safety issues by the carrying out of a formal and recorded risk assessment;

(c) consider the likely degree of intrusion for all those potentially affected;

(d) consider any adverse impact on community confidence that may result from the use or conduct of the CHIS or the information obtained; and

(e) ensure that records contain the required particulars of the CHIS and that these are not available except on a 'need to know' basis.

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

8.14 If an application is granted, the Authorising Officer must set a date for its review, and ensure that it is reviewed on that date (see 9.2 below). Records must be kept in relation to all RIPA applications and authorisations in accordance with paragraph 13 below, and to facilitate this, each investigation or operation should be given a unique reference number (URN) on the application form by the RIPA Monitoring Officer. Any subsequent forms (eg. renewals or cancellations) relating to the same investigation or operation should be identified by means of the same URN.

9. URGENT AUTHORISATIONS

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

10 DURATION OF AUTHORISATIONS

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

10.2 Authorisations should be reviewed at appropriate intervals in order to update the Authorising Officer on progress on the investigation and whether the authorisation is no longer required. Review periods should be set by the Authorising Officer, but should normally take place on a monthly basis unless the Authorising

Officer considers that they should take place more or less frequently (if so, the reasons should be recorded). If the surveillance provides access to confidential information or involves collateral intrusion, there will be a particular need to review the authorisation frequently. The results of reviews should be recorded on the appropriate form.

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

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

11 MATERIAL OBTAINED DURING INVESTIGATIONS

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

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

accordance with advice from the RIPA Monitoring Officer or the Senior Responsible Officer.

11.3 Where material obtained is of a confidential nature such as medical records or material covered by legal professional privilege then the following additional precautions should be taken:

• Confidential material should not be retained or copied unless it is necessary for a specified purpose;

• Confidential material should only be disseminated in accordance with legal advice that it is necessary to do so for a specific purpose;

• Confidential material which is retained should be marked with a warning of its confidential nature. Safeguards should be put in place to ensure that such material does not come into the possession of any person where to do so might prejudice the outcome of any civil or criminal proceedings;

• Confidential material should be destroyed as soon possible after its use for the specified purpose.

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

12 ASSESSMENT AND REVIEW

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

12.2 The cancellation form is available on the Council's website and should retain the same reference and be kept with the original RIPA paperwork

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

13 CCTV AND DIRECTED SURVEILLANCE

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

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

272. It is recommended that a law enforcement agency should obtain a written protocol with a local authority if the latter's CCTV system is to be used for directed surveillance. Any such protocol should be drawn up centrally in order to ensure a

unified approach. The protocol should include a requirement that the local authority should see the authorisation (redacted if necessary to prevent the disclosure of sensitive information) and only allow its equipment to be used in accordance with it.

13 RECORDS MANAGEMENT

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

13.2 A copy of all completed RIPA forms, including applications (whether granted or refused), authorisations, reviews, renewals and cancellations, must be forwarded by the Authorising Officer to the RIPA Administrator within five working days of the date of the relevant decision.

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

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

• any risk assessment in relation to the source;

• the circumstances in which tasks were given to the source;

• the value of the source to the investigating authority;

13.5 By law, an Authorising Officer must not grant authority for the use of a CHIS unless s/he believes that there are arrangements in place for ensuring that there is at all times a person with the responsibility for maintaining a record of the use made of the CHIS. Certain particulars must be included in the records relating to each CHIS, and the records must be kept confidential. Further advice should be sought from the RIPA Monitoring Officer or Senior Responsible Officer on this point if authority is proposed to be granted for the use of a CHIS.

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

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

14. ERROR REPORTING

14.1 The SRO will undertake a regular review of errors and a written record will be kept by the RIPA monitoring officer of each review.

14.2 Examples of errors are

-Surveillance or property interference activity has taken place without lawful authorisation.

-There has been a failure to adhere to the safeguards set out in the relevant statutory provisions and the Codes of Practice

-.a warrant or authorisation has been obtained as a result of the Council having been provided with information which later proved to be incorrect but on which the Council relied in good faith

14.3 All staff should inform the Authorising Officer of any error who will inform the RIPA Monitoring Officer within 3 working days of any error

14.4 If an error has occurred, the Council must notify the Investigatory Powers Commissioner as soon as reasonably practicable, and no later than ten working days. Where the full facts of the error cannot be ascertained within the timescale an initial notification must be sent with an estimated timescale for the error being reported in full and an explanation of the steps being undertaken to establish the full facts of the error. This must be followed up with a full report as outlined in paragraph 8.12 of the Covert Surveillance and Property Interference Code of Practice and any Investigatory Powers Commissioner Guidance.

15. NON-RIPA

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

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

15.3 Non-RIPA forms must be authorised by an Authorising Officer. However, if the activity relates to an investigation against a member of staff, authorisation must be provided by the Executive Director: Resources and Head of Paid Service. The same considerations and processes as set out in this policy in relation to RIPA authorisations should be followed save for the need for Magistrates approval.

16 TRAINING

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

16.2 Managers of enforcement teams must ensure that new staff undertake RIPA training within six months of their starting date.

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

APPENDIX A – ROLES AND RESPONSIBILITIES

Senior Responsible Officer – Tim O'Gara

RIPA Monitoring Officer –Sarah Sharland

RIPA Administrator – Rich Clark

AUTHORISING OFFICERS

Mike Jackson – Chief Executive Bristol City Council

Nick Carter –Head of Regulatory Services

Jonathan Martin- Trading Standards and Licensing Manager

Amy Kedward- Bristol Operations Centre Manager

Document is Restricted

Document is Restricted

Document is Restricted

Document is Restricted