Public Document Pack

Executive Member Decisions

Friday, 13th October, 2023
10.00 am

AGENDA

1. EMD RIPA UPDATE REPORT

Date Published: 13 October 2023
Denise Park, Chief Executive

EXECUTIVE MEMBER DECISION

REPORT OF:	Executive Member for Digital and Customer Services
LEAD OFFICERS:	Deputy Director Legal and Governance
DATE:	11 October 2023

PORTFOLIO/S AFFECTED:	Digital and Customer Services
WARD/S AFFECTED:	(All Wards);

SUBJECT: EMD RIPA UPDATE REPORT

1. EXECUTIVE SUMMARY

This is a report to the Executive Member to request approval of the amendments of the corporate RIPA Procedure and Guidance which is compliant both with the latest Home Office Statutory Codes of Practice and with recommendations of the Investigatory Powers Commissioner's Office made after their inspection in November last year**.**

2. RECOMMENDATIONS

That the Executive Member:

- Agrees to the amendments to the Procedure and Guidance see Appendix 1 showing the amendments in red and Appendix 2 is the final version clean copy.
- Note that the recommendations of the last inspection have been followed.

3. BACKGROUND

3.1 The Regulation of Investigatory Powers Act 2000 (RIPA) was introduced to provide a legal framework within which law enforcement agencies could undertake covert methods of investigation, namely, covert surveillance and the use of what are called 'covert human intelligence sources' (CHIS) lawfully. The main purpose of RIPA was to ensure that public authorities only interfered with an individual's human right to respect for their private and family life where it was necessary for the purposes of detection and prevention of crime and proportionate to their aims. This is a human right that is enshrined in the Human Rights Act 1998 and the European Convention on Human Rights. Examples of the types of offences that this Council investigates mainly for the purposes of public protection are trading standards offences (tobacco regulations, illegal puppy farming and trademarks infringements or underage sales), food safety and fly-tipping.

3.2 This legal framework consists of an internal system of authorisation. An investigating officer will complete an application form which is then submitted to the Authorising Officer appointed by

the Council who will decide whether or not to approve it. In the form the officer will set out why the proposed operation is lawful, necessary and proportionate. The law, definitions and guidance to enable this to be done, including the necessary forms to complete are set out in the Procedure and Guidance. This is then submitted to the Magistrates' Court for judicial approval.

3.3 This whole process is overseen by the Senior Responsible Officer (SRO) who is the Strategic Director of Resources and responsible for ensuring that corporate processes are being followed and also the RIPA Co-ordinator who is the Deputy Director Legal and Governance (Council Solicitor) who is responsible for ensuring compliance by ensuring the integrity of the processes whose duties include, organising training, overseeing the use of the powers internally and recording that use, error reporting and engagement with the IPCO for inspections**.**

3.4 There are quarterly meetings convened by the SRO of a group of officers who submit information as to whether any covert investigations have taken place or are likely to, and who assist to develop procedures and guidance in this area. The draft Procedure and Guidance was developed and worked up into this final form by the Group under the auspices of the SRO and the RIPA Co-ordinator.

3.5 On 17 July 2023 the Policy and Corporate Resources Overview and Scrutiny Committee (the Committee) was provided with an update on RIPA (Regulation of Investigatory Powers Act). The purpose of the report was to inform Members of any RIPA activity/applications, RIPA training delivered to officers, the compliance with recommendations of the Investigatory Powers Commissioner's Office (IPCO) and to approve the amendments of the latest Procedure and Guidance to ensure the compliance with the current RIPA Codes of Practice issued by the Home office and the Inspector's recommendations.

3.6 In November 2022 the Council was inspected by the IPCO – the Investigatory Powers Commissioner's Office. The Council's Strategic Director of Resources and Senior Responsible Officer (SRO), Principal Solicitor and RIPA Co-ordinating Officer (RCO), were interviewed by the Inspector using video conferencing facilities. Supporting documentation requested by the Inspector was supplied. Also present at the interview were Deputy Director, Legal and Governance and Service Lead, Public Protection and Environmental Health, one of the Council's Authorising Officers.

3.7 In his letter of 17 November 2022 the Inspector praised the Council's Procedure and Guidance and he suggested a some amendments which have now been made. The Inspector noted that whilst the Council had not exercised its RIPA powers for a significant period of time, he said it was 'pleasing' to hear that the authorising officer cadre, together with those officers most likely to engage the powers, received "desk top" training last year. This took place on 15 December 2021 and 27 January 2022 and was run by the Council's Service Lead Public Protection and Principal Solicitor – Litigation and Authorising Officer.

3.8 The Inspector was also informed that a web-based training video on the Council's intranet is under development and will assist to raise RIPA awareness.

3.9 The Inspector inspected the very last authorisation and stated that it had been completed to a high standard by Service Lead Public Protection the authorising officer.

3.10 The Council agreed to take the following steps to comply with the IPCO recommendations:

- to introduce a system whereby all social media and internet research is overseen by the RIPA Officer's Group every three months.
- to ensure material acquired under RIPA and the Investigatory Powers Act is properly retained, reviewed, and ultimately destroyed by all participants in the RIPA process including investigating officers, manager and authorising officers and
- to add appropriate wording to the RIPA Procedure and Guidance so that it provides practical guidance on the retention, review and destruction of RIPA authorisations.

3.11 It is to be noted that the Council normally prefers to employ the use of overt investigatory techniques but with local authorities in general the IPCO Inspector was mainly concerned that in not using these available powers Council employees would become unskilled in recognising when they may be inadvertently using covert human intelligence sources without the correct processes. The desk top training referred to above was designed to address this.

3.12 The RIPA Procedure and Guidance with its amendments in red is at Appendix 1 and the final version clean copy is at Appendix 2.

4. KEY ISSUES & RISKS

This Procedure and Guidance will assist to increase awareness amongst Council officers and ensure compliance with the Human Rights Act 1998. The Council is obliged to adopt the new RIPA Procedure and Guidance to ensure it is compliant with current Home Office Codes of Practice and to enable it to produce it to the IPCO at the next inspection which is likely to be this year. The Council needs to ensure its internet research and social media access activity, albeit limited, is monitored by the RIPA Group quarterly. It also needs to adopt the amendments to the RIPA Procedure and Guidance to ensure it is compliant with current guidance and to enable it to produce up to date documentation to the IPCO at the next inspection which is likely to be in 2025.

5. POLICY IMPLICATIONS

This Procedure and Guidance is being amended. It is not a change of policy.

6. FINANCIAL IMPLICATIONS

There are no financial implications.

7. LEGAL IMPLICATIONS

Adoption of the amendments of the Procedure and Guidance is essential in order to show compliance with the latest Home Office Codes of Practice.

8. RESOURCE IMPLICATIONS

There are no resource implications.

9. EQUALITY AND HEALTH IMPLICATIONS
Please select one of the options below. Where appropriate please include the hyperlink to the EIA.

Option 1 ☒ Equality Impact Assessment (EIA) not required – the EIA checklist has been completed.

Option 2 ☐ In determining this matter the Executive Member needs to consider the EIA associated with this item in advance of making the decision. *(insert EIA link here)*

Option 3 ☐ In determining this matter the Executive Board Members need to consider the EIA associated with this item in advance of making the decision. *(insert EIA attachment)*

10. CONSULTATIONS
Internal consultations have been carried out at the RIPA group meetings with departmental representatives and external consultations are not required.

11. STATEMENT OF COMPLIANCE
The recommendations are made further to advice from the Monitoring Officer and the Section 151 Officer has confirmed that they do not incur unlawful expenditure. They are also compliant with equality legislation and an equality analysis and impact assessment has been considered. The recommendations reflect the core principles of good governance set out in the Council's Code of Corporate Governance.

12. DECLARATION OF INTEREST
All Declarations of Interest of any Executive Member consulted and note of any dispensation granted by the Chief Executive will be recorded and published if applicable.

VERSION:	**1**

CONTACT OFFICER:	**Shelagh Lyth**
DATE:	18 August 2023
BACKGROUND PAPER:	Available on request

Regulation of Investigatory Powers Act 2000 **(RIPA)**

Procedure and Guidance

PHF 4 July 2019 ADAPTED BY SJL FOR BWDC 2021 Amended 2023

Contents

PART A Introduction & RIPA General

1. Introduction

1.1 The performance of certain investigatory functions of local authorities may require the surveillance of individuals or the use of undercover officers and informants. Such actions may intrude on the privacy of individuals and can result in private information being obtained and as such, should not be undertaken without full and proper consideration. The Regulation of Investigatory Powers Act 2000 (RIPA) governs these activities and provides a means of ensuring that they are carried out in accordance with law and subject to safeguards against abuse.

All surveillance activity can pose a risk to local authorities from challenges under the HRA or other processes. Therefore, all staff involved in the process shall take their responsibilities seriously so as to enhance the integrity of these processes, procedures and oversight responsibilities which have been adopted by Blackburn with Darwen Borough Council (the Council).

This Procedural Guidance follows the RIPA Codes of Practice. This version of the Procedural Guidance will replace the previous version on the date referred to in the version control table.

If having read this document you are unclear about any aspect of the process, seek the advice from the RIPA Co-ordinator.

2. Scope of this Procedural Guidance (Guidance)

2.1 The purpose of this Procedure and Guidance (Guidance) is to provide a consistent approach to the authorisation and undertaking of surveillance activity that is carried out by the Council. This includes the use of undercover officers and informants, known as Covert Human Intelligence Sources (CHIS). This will ensure that the Council complies with the Regulation of Investigatory Powers Act 2000 (RIPA).

2.2 The Guidance sets out the Council's procedure for the authorisation processes and the roles of the respective staff involved.

2.3 The Guidance also sets out the Council's procedure relating to surveillance which is considered necessary in the public interest to be undertaken by the authority but cannot be authorised under the RIPA legislation. This type of surveillance will have to be compliant with the Human Rights Act and is referred to as 'Non-RIPA'. (See para 21).

2.4 The Guidance also identifies how it fits with other guidance, policies and legislation, particularly with the Human Rights Act 1998, GDPR/Data Protection Act 2018 and the Criminal Procedure and Investigations Act 1996.

2.5 All RIPA covert activity will have to be authorised and conducted in accordance with this Guidance, the RIPA legislation and the Home Office Codes of Practice. Therefore, all officers involved in the process will have regard to this document and the statutory RIPA Codes of Practice issued and updated from time to time under section 71 RIPA (current version issued in December 2022) for both Directed Surveillance and the use of Covert Human Intelligence Sources (CHIS). This is a link to the 2 Codes of Practice:

RIPA codes - GOV.UK (www.gov.uk)

3. Background to RIPA and Lawful Criteria

3.1 On 2nd October 2000 the Human Rights Act 1998 (HRA) came into force. Section 6 states that it is unlawful for a public authority to act in a way which is incompatible with a Convention right. This makes it unlawful for a local authority to breach any article of the European Convention on Human Rights (ECHR).

3.2 Article 8 of the European Convention on Human Rights is set out below:

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.

3.3 The right under Article 8 is a qualified right and public authorities can interfere with this right for the reasons given in 3.2 (2) above if it is necessary and proportionate to do so.

3.4 Those who undertake Directed Surveillance or CHIS activity on behalf of a local authority may not breach an individual's Human Rights, unless such surveillance is **lawful,** consistent with Article 8 of the ECHR and is both **necessary (**see section 42**)** and **proportionate** (see section 43) to the matter being investigated.

3.5 RIPA provides a legal framework for justified interference by law enforcement authorities to ensure that any such activity undertaken, together with the information obtained, is HRA compatible and lawful.

3.6 However, under RIPA, local authorities can now only authorise Directed Surveillance for the purpose of preventing or detecting conduct which constitutes a criminal offence which is punishable (whether on summary conviction or indictment) by a maximum

term of at least six months imprisonment; (serious crime criteria) or involves the illegal sale of alcohol or tobacco to children. (See Sec 14 re 'lawful grounds)

3.7 The lawful criteria for CHIS authorisation is also prevention and detection of crime and prevention of disorder **BUT** the offence investigated is not limited to those that carry a sentence of 6 months imprisonment.

3.8 Furthermore, the Council's authorisation of Directed Surveillance or use of CHIS can only take effect with judicial approval which means it can only take place once a court order approving the authorisation has been granted by a Justice of the Peace (JP).

3.9 RIPA ensures that any surveillance and use of CHIS which is undertaken following a correct authorisation and approval from a Justice of the Peace is lawful. Therefore, it protects the authority from legal challenge. It also renders any activity authorised under RIPA and the evidence obtained by that means 'lawful for all purposes'.

4. Consequences of Not Following RIPA

4.1 Although not obtaining authorisation does not make the authorisation unlawful per se, it does have some consequences: -

- Evidence that is gathered may be inadmissible in court;
- The subjects of surveillance can bring a claim against the local authority for breach of their Article 8 rights which could be costly;
- Reputational damage as well as financial loss – especially If a challenge under Article 8 is successful;
- Any person who believes that their rights have been breached can have their complaint dealt with by the Investigatory Powers Tribunal (IPTC) (See Complaints section 66)
- The activity could be construed as an error and therefore have to be investigated and a report submitted by the Senior Responsible Officer to the Investigatory Powers Commissioner's Office (IPCO). (See Sec 65 Errors)

4. Independent Oversight

5.1 From 1 Sept 2017 oversight was given to the **Investigatory Powers Commissioner's Office (IPCO**). They are the independent inspection office whose remit includes providing comprehensive oversight of the use of the powers to which the RIPA code applies, and adherence to the practices and processes described in it. They also provide guidance to be followed which is separate to the codes. Their main oversight duties are set out in section 229 of the Regulation of Investigatory Powers Act 2016.

5.2 The 2016 Act gives them unfettered access to all locations, documentation and information systems as is necessary to carry out their full functions and duties and they will periodically inspect the records and procedures of the Council to ensure the appropriate authorisations have been given, reviewed, cancelled, and recorded properly.

5.3 It is the duty of any person who uses these powers to comply with any request made by a Commissioner to disclose or provide any information they require for the purpose of enabling them to carry out their functions. Therefore, it is important that the Council can show it complies with this Guidance and with the provisions of RIPA 2000 and 2016.

PART B Surveillance, Types and Criteria

6. Introduction

6.1 It is important to understand the definition of surveillance and what activities are classed as surveillance under RIPA. Surveillance can be both overt and covert but not all surveillance can be authorised under RIPA and so become 'lawful for all purposes'. There are also different degrees of authorisation depending on the circumstances.

7. Surveillance Definition

7.1 **Surveillance is:**

- Monitoring, observing or listening to persons, their movements, their conversations or their other activities or communications.
- Recording anything monitored, observed or listened to in the course of surveillance,
- Surveillance by means of a surveillance device.

8. Overt Surveillance

8.1 Overt surveillance is where the subject of surveillance is aware that it is taking place, either by way of signage such as in the use of CCTV or because the person subject of the surveillance has been informed of the activity.

8.2 Overt surveillance is outside the scope of RIPA and therefore does not require authorisation. However, it still must take account of privacy under the Human Rights

Act 1998 and be necessary and proportionate. Any personal data obtained will also be subject of the Data Protection Act.

9. Covert Surveillance

9.1 Covert Surveillance is defined as "surveillance which is carried out in a manner calculated to ensure that the persons subject to the surveillance are unaware that it is or may be taking place" and is covered by RIPA. Covert surveillance is categorised as either **intrusive** or **directed.**

9.2 There are three categories of covert surveillance regulated by RIPA: -

1) **Intrusive surveillance** (Local Authorities are not permitted to carry out intrusive surveillance).

2) **Directed Surveillance;**

3) **Covert Human Intelligence Sources** (CHIS).

10. Intrusive Surveillance

10.1 Blackburn with Darwen Borough Council has no authority in law to carry out Intrusive Surveillance. Only the Police and other central government law enforcement agencies can lawfully carry out intrusive surveillance.

10.2 Intrusive surveillance is defined in section 26(3) of the 2000 Act as

- covert surveillance which
- Is carried out in relation to anything taking place on any residential premises or in any private vehicle; and
- Involves the presence of an individual on the premises or in the vehicle or is carried out by means of a surveillance device.

10.3 Where surveillance is carried out in relation to anything taking place on any residential premises or in any private vehicle by means of a device, without that device being present on the premises, or in the vehicle, it is not intrusive unless the device consistently provides information of the same quality and detail as might be expected to be obtained from a device actually present on the premises or in the vehicle. Thus, an observation post outside premises, which provides a limited view and no sound of what is happening inside the premises, would not be considered as intrusive surveillance.

10.4 The capability of equipment being used for surveillance on residential premises and private vehicles, such as high-powered zoom lenses, should be considered to ensure that its use does not meet the criteria of Intrusive Surveillance.

11. Directed Surveillance Definition

11.1 The Council can lawfully carry out Directed Surveillance for the prevention and detection of crime and prevention of disorder where the crime is punishable by imprisonment of 6 months or is relating to the illegal sale of tobacco or alcohol to children. However, surveillance is only Directed Surveillance if the following are all true:

- It is covert, but not intrusive surveillance;
- It is conducted for the purposes of a specific investigation or operation;
- It is likely to result in the obtaining of private information (see private information below) about a person (whether or not one specifically identified for the purposes of the investigation or operation);
- It is conducted otherwise than by way of an immediate response to events or circumstances the nature of which is such that it would not be reasonably practicable for an authorisation to be sought.

12. Private information

12.1 By its very nature, surveillance may involve invading an individual's right to privacy. The level of privacy which individuals can expect depends upon the nature of the environment they are in at the time. For example, within an individual's own home or private vehicle, an individual can expect the highest level of privacy. The level of expectation of privacy may reduce if the individual transfers out into public areas.

12.2 The Codes of Practice provide guidance on what is private information. They state that private information includes any information relating to a person's private or family life. As a result, private information is capable of including any aspect of a person's private or personal relationship with others, such as family and professional or business relationships.

12.3 Whilst a person may have a reduced expectation of privacy when in a public place, covert surveillance of that person's activities in public may still result in the obtaining of private information. This is likely to be the case where that person has a reasonable expectation of privacy even though acting in public and where a record is being made by a public authority of that person's activities for future consideration or analysis. Surveillance of publicly accessible areas of the internet should be treated in a similar

way, recognising that there may be an expectation of privacy over information which is on the internet, particularly where accessing information on social media websites.

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

12.5 Private information may include personal data, such as pictures of a person's face, names, telephone numbers, car registration numbers and address details. Where such information is acquired by means of covert surveillance of a person having a reasonable expectation of privacy, a Directed Surveillance authorisation is appropriate.

12.6 Information which is non-private may include publicly available information such as, books, newspapers, journals, TV and radio broadcasts, newswires, websites, mapping imagery, academic articles, conference proceedings, business reports, photographs, videos and more. Such information may also include commercially available data where a fee may be charged, and any data which is available on request or made available at a meeting to a member of the public.

12.7 There is also an assessment to be made regarding the risk of obtaining collateral intrusion which is private information about persons who are not subjects of the surveillance (see section 44).

13. Confidential or Privileged Material

13.1 This is defined in the Codes of Practice as material that has the quality of confidence in common law and in particular reference is made to confidential journalistic material and sources of journalistic information, other confidential personal information such as medical records or spiritual counselling, confidential discussions between Members of Parliament and their constituents and also matters subject to legal privilege.

13.2 Particular consideration should be given in cases where the subject of the investigation or operation might reasonably assume a high degree of confidentiality. This includes where the material contains information that is legally privileged, confidential journalistic material or where material identifies a journalist's source, where material contains confidential personal information or political information such as communications between a Member of Parliament and another person on constituency business.

13. 3 According to the Annex to the Codes of Practice, Directed Surveillance likely or intended to result in the acquisition of knowledge of confidential or privileged material must be

authorised by the 'Head of Paid Service' who is the Council's **Chief Executive who must seek legal advice from the RIPA Co-Ordinator prior to authorisation.**

13.2 Advice should be sought from the RIPA Co-Ordinator by investigating officers at the earliest stage if there is a likelihood of obtaining this type of material.

14. Lawful Grounds

14.1 Authorisation for Directed Surveillance cannot be given unless it is to be carried out for the purpose of preventing or detecting a criminal offence(s) and it meets the serious crime test i.e. that the criminal offence which is sought to be prevented or detected is

1) Punishable, whether on summary conviction or on indictment, by a maximum term **of at least 6 months of imprisonment**, or,

2) Would constitute an offence under sections 146, 147 or 147A of the Licensing Act 2003 or section 7 of the Children and Young Persons Act 1933 (see 1.4 above) – sale of alcohol or tobacco to children.

14.2 Preventing or detecting crime goes beyond the prosecution of offenders and includes actions taken to avert, end or disrupt the commission of criminal offences.

14.3 For CHIS authorisations the lawful grounds are the same in that it is to be carried out for the purpose of preventing or detecting a criminal offence(s) **BUT NB it does not have to meet the serious crime test. (cf para 3.7)**

15. Test Purchases

15.1 Test purchase activity does not in general require authorisation as a CHIS under RIPA as vendor-purchaser activity does not normally constitute a relationship as the contact is likely to be so limited. However, if a number of visits are undertaken at the same establishment to encourage familiarity, a relationship may be established and authorisation as a CHIS should be considered. If the test purchaser is wearing recording equipment and is not authorised as a CHIS, or an adult is observing, consideration will be given as to whether in any particular case a Directed Surveillance authorisation should be granted. There is an example in the current Directed Surveillance Code of Practice (para 3.33) of an underage test purchaser of alcohol wearing a surveillance device or being observed by an adult and it recommends that *consideration should be given to granting a directed surveillance authorisation.*

15.2 Note that an authorisation is only needed where the surveillance meets the Directed Surveillance threshold namely, covert surveillance in a situations where you are likely to obtain private information.

15.3 Remember that it is only where the offence carries a maximum sentence of 6 months imprisonment or involves the sale of alcohol or tobacco to children that RIPA will apply.

If it does not meet that threshold or it is decided not to apply for an authorisation, it is important that a full written risk assessment is done in which the activity is justified from the aspect of compliance with Article 8 and section 6 of the Human Rights Act 1998. In addition, in all cases which are outside the scope of RIPA the Authorising Officer should consider the use of a non-RIPA application for this where it is likely that private information will be obtained as a way to achieve and show compliance.

15.4 When conducting covert test purchase operations at more than one establishment, it is not necessary to construct an authorisation for each premise to be visited but the intelligence must be sufficient to prevent “fishing trips”. Premises may be combined within a single authorisation provided that each is identified at the outset. Necessity, proportionality, and collateral intrusion must be carefully addressed in relation to each of the premises.

15.5 NB. It is unlikely that authorisations will be considered proportionate without demonstration that overt methods have been considered or attempted and failed. Adequate reasons for not using or not attempting overt methods will be needed.

16. Urgent cases

16.1 Since 1 November 2012 there has been no provision to enable urgent oral authorisations to be given under RIPA as all authorisations now have to be approved by a Justice of the Peace which takes time. If any surveillance within the definition of Directed Surveillance was required to be carried out in an urgent situation or as an immediate response, this could still take place but only outside RIPA – as a ‘Non-Ripa’- in exceptional cases provided that it could be shown to be justified as necessary and proportionate in accordance with Article 8 ECHR and the Human Rights Act 1998. (see section 21 below). Should it ever appear to an Investigating Officer that an urgent oral Non RIPA authorisation is required he should contact an Authorising Officer who will consider the legality, necessity and proportionality when deciding whether to grant it orally. Once granted the AO must make a formal note of the reasons for the decision using a non-RIPA form as a template and place it on the file of the case and provide a copy for the RIPA Co-ordinator and Senior Responsible Officer as soon a reasonably practicable.

17. Surveillance for Preventing Disorder

17.1 Authorisation for the purpose of preventing disorder can only be granted if it involves a criminal offence(s) punishable (whether on summary conviction or indictment) by a maximum term of at least 6 months' imprisonment. Surveillance for disorder not meeting these criteria would need to be carried out as surveillance outside of RIPA in accordance with the Non-RIPA procedure. (See below)

18. CCTV

18.1 CCTV is now known as a Surveillance Camera System Section 29(6) Protection of Freedoms Act 2012. "Surveillance camera systems" is taken to include:

(a) closed circuit television (CCTV) or automatic number plate recognition (ANPR) systems;

(b) any other systems for recording or viewing visual images for surveillance purposes;

18.2 The Surveillance Camera Code of Practice 2013 (as amended in 2021) defines a 'surveillance camera system' as having the meaning given by Section 29(6) of PoFA 2012 and is taken to include:

(a) closed circuit television (CCTV) or automatic number plate recognition (ANPR) systems;

(b) any other systems for recording or viewing visual images for surveillance purposes;

(c) any systems for storing, receiving, transmitting, processing or checking the images or information obtained by (a) or (b); (d) any other systems associated with, or otherwise connected with (a), (b) or (c)

This includes

- CCTV, Body Worn Video (BWV) and dash cams,
- Automatic Number Plate Recognition;
- Deployable mobile overt mobile camera systems e.g. to observe fly-tipping sites.
- Any other system for recording or viewing visual images for surveillance purposes;
- Any systems for storing, receiving, transmitting, processing or checking images or information obtained by those systems; and
- Any other systems associated with, or otherwise connected with those systems.

18.3 The use of CCTV systems operated by the Council do not normally fall under the RIPA regulations. However, they are also governed by the Data Protection Act 2018, Protection of Freedoms Act 2012 and the Surveillance Camera Code 2013 (as amended in 2021) issued by the Surveillance Camera Commissioner. In addition, they are governed by guidance issued by the Information Commissioner's Office (ICO) available on their website and the Council's CCTV Code of Practice also available on the Council's website.

18.4 Should there be a requirement for the CCTV cameras to be used to conduct surveillance for a different and/or another specific purpose or operation than the one they were originally set up for it is likely that the activity will fall under Directed Surveillance and therefore require an authorisation. Therefore, operators of the

Councils CCTV system need to be aware of the RIPA issues associated with using CCTV and that continued, prolonged systematic surveillance of an individual or spaces where targeted individuals frequent may require an authorisation.

18.5 On the occasions when the CCTV cameras are to be used in a Directed Surveillance situation either by enforcement officers from relevant departments within the Council or outside Law Enforcement Agencies such as the Police, CCTV staff should always be supplied with an assurance in writing (e.g. by official e-mail from the organisation concerned) that there is a RIPA authorisation in place, what it is for, the name and rank of the authorising officer and also the expiry date. A copy of the authorisation form in a redacted format, or a copy of the authorisation page could be requested in some cases if it is considered by the operators of the CCTV system to be necessary. If it is an urgent oral authority from the Police, a copy of the applicant's notes are to be retained or at least some other document in writing which confirms the authorisation and exactly what has been authorised. It is important that the staff check the authority and only carry out what is authorised. This information is also to be forwarded to the Central Record kept by the RIPA Co-Ordinator filing. This will assist the Council to evaluate the authorisations and assist with oversight.

19. Automatic Number Plate Recognition (ANPR)

19.1 Automated Number Plate Recognition (ANPR) does not engage RIPA if it is used for the purpose it is registered for, such as traffic flow management or safety and enforcement within car parks. However, it is capable of being a surveillance device if used in a pre-planned way to carry out surveillance by monitoring a particular vehicle by plotting its locations, e.g. in connection with illegally depositing waste (fly-tipping).

19.2 Should it be necessary to use any ANPR systems to monitor vehicles, RIPA principles of lawfulness necessity and proportionality apply and a Directed Surveillance Authorisation should be sought.

20 Internet and Social Media Investigations

20.1 Online open source research is widely regarded as the collection, evaluation and analysis of material from online sources available to the public, whether by payment or otherwise to use as intelligence and evidence.

20.2 The use of online open source internet and social media research techniques has become a productive method of obtaining information to assist local authorities with their regulatory and enforcement functions. It can also assist with service delivery issues and debt recovery. However, the use of the internet and social media is constantly evolving and with it the risks associated with these types of enquiries, particularly regarding breaches of privacy under Article 8 Human Rights Act (HRA) and other operational risks.

20.3 The internet is another method of carrying out surveillance (defined in section 7) and that makes a computer 'a surveillance device'. Repeated viewing of 'open source' sites for the purpose of intelligence gathering and data collation on one individual and their family may constitute Directed Surveillance or if outside the definition and outside RIPA it could constitute a breach of Article 8 ECHR. Activities of monitoring through, for example, a Facebook profile for a period of time where a record of the information is kept for later analysis or evidential purposes is likely to require a RIPA authorisation if it is done to obtain evidence of a crime carrying over 6 months imprisonment. If it is outside RIPA a Non-RIPA form should be completed. Where covert contact is made with another person on the internet a CHIS authority may be required.

20.4 Where the activity falls within the criteria of surveillance or CHIS outside of RIPA, again this will require authorising as a 'non RIPA' matter on a Non-RIPA form which will be authorised by the RIPA Authorising Officers listed in appendix B.

20.5 **NB** There is more specific guidance that covers online open source research which should be read and followed in conjunction at **Appendix A** of this Guidance headed, **'Internet and Social Media Research and Investigations Guidance'**.

21. Surveillance Outside of RIPA i.e. 'Non RIPA'

21.1 Compliance with RIPA provides a legal 'shield' because, rather like an insurance policy, properly authorised Directed Surveillance is 'lawful for all purposes' and will provide a defence against a claim for breach of Article 8.

21.2 In order to take advantage of that 'shield' Directed Surveillance must be for the purpose of prevention and detection of crime and prevention of disorder and the criminal offence concerned must carry **a 6-month prison sentence** (Directed Surveillance crime threshold) or relate to the sale of alcohol or tobacco to children.

21.3 Some investigations relate to offences that do not meet this threshold and yet, it may still considered necessary to undertake surveillance. Examples include:

- Surveillance for anti-social behaviour disorder which do not attract a maximum custodial sentence of at least six months imprisonment.
- Planning enforcement prior to the serving of a notice or to establish whether a notice has been breached.
- Most licensing breaches.
- Safeguarding vulnerable people (where it is clear that the evidence does not indicate a criminal offence e.g. child neglect under section 1 of the Children and Young Persons Act 1933).
- Civil matters such as insurance claims.
- Disciplinary surveillance (see below).

21.4 So in cases like those, where the surveillance is of an individual who is unaware they are being monitored or observed and it not possible to engage the RIPA 'shield' there

is a higher risk that this activity could breach someone's article 8 rights to privacy. Therefore, the activity should be conducted in way which is HRA compliant, which will include considering whether the activity is lawful, necessary and proportionate.

21.5 S**taff disciplinary surveillance** such as poor time-keeping or other non-criminal matters must be compliant with the Monitoring at Work Guidance issued by the Information Commissioner's Office. This is to ensure that is complies with the HRA and the GDPR.

21.6 Should the investigation also involve a criminal offence which meets the RIPA criteria such as theft or fraud, and it is intended to prosecute the offender, the option to carry out the surveillance under RIPA should be considered so as to engage the RIPA 'shield'. However, it must be planned as a genuine criminal investigation with a view to prosecution.

21.7 Should it be necessary to undertake disciplinary surveillance, advice should be sought from the RIPA Co-Ordinator.

21.8 As part of the process of formally recording and monitoring non-RIPA surveillance, a non-RIPA surveillance application form should be completed and authorised by an Authorising Officer. A template application form can be obtained from the RIPA Co-Ordinator.

21.9 The Senior Responsible Officer (see 37 below for responsibilities etc) will maintain an oversight of non-RIPA surveillance to ensure that such use is compliant with Human Rights and other relevant legislation. The RIPA Co-Ordinator will maintain a Central Record of non-RIPA surveillance in addition to the required Central Records for Directed Surveillance and CHIS (see para 55 and 56).

21.10 The RIPA codes also provide guidance that authorisation under RIPA is not required for the following types of activity:

- General observations – see examples in section 3.33 in the codes of practice that do not involve the systematic surveillance of an individual or a group of people and should an incident be witnessed the officer will overtly respond to the situation. This is not within the definition of surveillance.
- Use of overt CCTV and overt Automatic Number Plate Recognition systems. This is not covert so outside the definitions of directed and intrusive surveillance.
- Surveillance where no private information is likely to be obtained. This is also outside the definitions of directed and intrusive surveillance.
- Surveillance undertaken as an immediate response to a situation. This is a situation specifically excluded from the definition of directed surveillance.
- Covert surveillance relating to a criminal offence other than one which is within the RIPA criteria.
- The use of a recording device by a CHIS in respect of whom an appropriate use or conduct authorisation has been granted permitting them to record any information in their presence. This is covered by the parameters set within the CHIS authorisation.

- The covert recording of noise where the recording is of decibels only or constitutes non-verbal noise (such as music, machinery or an alarm), or the recording of verbal content is made at a level which does not exceed that which can be heard from the street outside or adjoining property with the naked ear. In the latter circumstance, the perpetrator would normally be regarded as having forfeited any claim to privacy. In either circumstance this is outside of RIPA. This is because this does not constitute private information.

21.11 Where it is deemed necessary to undertake an investigation to which RIPA is not applicable but it does involve undertaking covert surveillance in a way that is directed at an individual for a specific investigation over a period of time, if the officer is concerned that private information is going to be gathered it is recommended that the officer concerned completes a NON-RIPA application form.

22. Joint Agency Surveillance

22.1 In cases where one agency is acting on behalf of another, it is usually for the tasking agency to obtain or provide the authorisation. For example, where surveillance is carried out by Council employees on behalf of the Police, authorisation would be sought by the Police. If it is a joint operation involving both agencies, the lead agency should seek authorisation.

22.2 Council staff involved with joint agency surveillance are to ensure that all parties taking part are authorised on the RIPA authorisation form to carry out the activity. When staff are operating on another organisation's authorisation they are to ensure they see what activity they are authorised to carry out and make a written record. They should also provide a copy of the authorisation to the RIPA Co-Ordinator. This will assist with oversight of the use of Council staff carrying out these types of operations. Line Managers should be made aware if their staff are involved in this type of surveillance.

23. Use of Third-Party Surveillance

23.1 In some circumstances it may be appropriate or necessary for Blackburn with Darwen Borough Council to work with third parties who are not themselves a Public Authority (such as an individual, company or non-governmental organisation) to assist with an investigation. Where that third party is acting in partnership with or under the direction of the Council, then they are acting as our agent and any activities that the third party, or the individuals employed by that third party, carry out which meet the RIPA definitions of Directed Surveillance should be authorised. This is because the agent or employee carrying out the activity will be subject to RIPA in the same way as any employee of the Council would be. The Council should ensure that any agents they instruct are properly qualified, understand RIPA obligations and understand they could be inspected by the IPCO, have clean DBS certificates, are ICO registered for data protection purposes and have the necessary skills to achieve the objectives. Note that such agents must be certified by a UKAS accredited certification body to the current edition of BS102000 and are inspected annually so this is a simple check that can be done. If advice is required, please contact the RIPA Co-Ordinator.

23.2 Similarly, a surveillance authorisation should also be considered where the Council is aware that a third party (that is not a Public Authority) is independently conducting surveillance and the Council intends to make use of any suitable material obtained by the third party for the purposes of a specific investigation.

24. Surveillance Equipment

24.1 The Council will maintain a central (asset) register of all surveillance equipment such as cameras and noise monitoring devices. This will require a description, Serial Number, an explanation of its capabilities and where it is stored.

24.2 The register will be held and maintained by the RIPA Co-Ordinator. The equipment will be stored securely by the issuing department.

24.3 All equipment capable of being used for Directed Surveillance such as cameras etc. should be properly maintained and fit for purpose for which they are intended.

24.4 When completing an Authorisation, the applicant must provide the Authorising Officer with details of any equipment to be used and its technical capabilities. The Authorising Officer will have to take this into account when considering the intrusion issues, proportionality and whether the equipment is fit for the required purpose. The Authorising Officer must make it clear on the Authorisation exactly what equipment if any they are authorising and in what circumstances.

PART C. Covert Human Intelligence Sources (CHIS)

25. Introduction

25.1 A RIPA authorisation can also be obtained for the use of Covert Human Intelligence Sources (CHIS). These are sources commonly known as informants (members of the public providing the Council with information), and the activities of undercover officers. They can be employees of the Council, agents or members of the public engaged by the Council to establish or maintain a covert relationship with someone to in order to obtain information.

25.2 Unlike directed surveillance, which interferes with Article 8 on the basis that it is likely to result in obtaining information relating to a person's private or family life, CHIS relationships may amount to an interference regardless of whether such private information is obtained. This is on the basis that Article 8 protects the right to establish and develop relationships (both personal and professional). Covert manipulation of a relationship by a public authority (e.g. where one party has a covert purpose and is acting on behalf of a public authority) may therefore engage Article 8, regardless of whether private information is obtained.

25.3 Not all human source activity will meet the definition of a CHIS. For example, a source may be a public volunteer or someone who discloses information out of professional or statutory duty or has been tasked to obtain information other than by way of a covert

relationship. However, Officers must be aware that volunteers giving information may have obtained that information in the course of an ongoing relationship with a family member, friend, neighbour or business associate. The Council has a duty of care to all members of the public who provide information to us and appropriate measures must be taken to protect that source. How the information was obtained should be established to determine the best course of action. The source and information should also be managed correctly in line with CPIA and the disclosure provisions.

25.4 Recognising when a source becomes a CHIS is therefore important as this type of activity may need authorisation. Council employees must ensure that their daily interaction with members of the public does not inadvertently cross-over into CHIS territory. For example, if a member of the public makes a complaint about antisocial behaviour, they should not be asked to utilise a relationship with a person covertly to obtain information about possible criminal offences because this amounts to the tasking of a CHIS. Should a CHIS authority be required, all of the staff involved in the process should make themselves fully aware of the contents of this Procedural Guidance and the CHIS codes of Practice. (see link to Codes at 2.5)

25.5 Council employees should make themselves aware of the definition of a CHIS – para 26 below - to ensure that this cross-over never occurs without first obtaining of a CHIS authorisation and all the accompanying safeguards are in place.

25.6 A CHIS, their conduct, and the use to which they are put is defined within Section 26(7) and (8) of RIPA. Chapter 2 of the relevant Code also provides examples of where this regime may apply.

25.7 Legal advice from the RIPA Co-Ordinator should always be sought where consideration is to be given to the use of CHIS.

26. Definition of CHIS

26.1 Individuals act as a covert human intelligence sources (CHIS) if they:

i) establish or maintain a covert relationship with another person to obtain information.

ii) covertly give access to information to another person, or

iii) disclose information covertly which they have obtained using the relationship or they have obtained because the relationship exists.

26.2 A relationship is established, maintained or used for a covert purpose if and only if it is conducted in a manner that is **calculated to ensure that one of the parties to the relationship is unaware of the purpose.** This does not mean the relationship with the Council Officer/Handler and the person providing the information, as this is not covert. It relates to how the information was either obtained or will be obtained. **Was it or will it be obtained from a third party without them knowing it was being passed on to the Council?** This would amount to a covert relationship.

26.3 It is possible, that a person will become engaged in the conduct of a CHIS without a public authority inducing, asking or assisting the person to engage in that conduct. An

authorisation should be considered, for example, where a public authority is aware that a third party is independently maintaining a relationship (i.e. “self-tasking”) in order to obtain evidence of criminal activity and the public authority intends to make use of that material for its own investigative purposes. (Section 2.26 Codes of CHIS Codes of Practice

27. Vulnerable and Juvenile CHIS

27.1 Special consideration must be given to the use of a Vulnerable Individual as a CHIS. A ‘vulnerable individual’ is a person who is or may be in need of community care services by reason of mental or other disability, age or illness and who is or may be unable to take care of himself, or unable to protect himself against significant harm or exploitation. Any individual of this description, or a juvenile as defined below, should only be authorised to act as a source in exceptional circumstances and only then when authorised by the Chief Executive.

27.2 Special safeguards also apply to the use or conduct of juvenile sources; that is sources under the age of 18 years. On no occasion should the use or conduct of a source under 16 years of age be authorised to give information against his parents or any person who has parental responsibility for him.

27.3 If the use of a vulnerable individual or a juvenile is being considered as a CHIS you must consult the RIPA Co-ordinator before authorisation is sought as authorisations should not be granted in respect of a juvenile CHIS unless the special provisions contained within the Regulation of Investigatory Powers (Juveniles) Order 2000; SI No. 2793 are satisfied and an enhanced risk assessment is undertaken.

27.4 NB Local authorities are not permitted to give criminal conduct authorisations under any circumstances whether the CHIS is a juvenile or not.

28. CHIS Criteria

28.1 The lawful criteria for CHIS authorisation is prevention and detection of crime and prevention of disorder. **NB The serious crime criteria of the offence carrying maximum penalty a 6-month sentence etc. does NOT apply to CHIS.**

28.2 Authorisations for juvenile sources must be authorised by the Chief Executive of the Council (or, in their absence, the Deputy Chief Executive).

28.3 All authorisations for use of CHIS must be ratified by a Justice of the Peace at a magistrates’ court.

29. Use and Conduct of a Source

29.1 The way the Council would use a CHIS for covert activities is known as 'the use and conduct' of a source.

29.2 The **use** of a CHIS involves any action on behalf of a public authority to induce, ask or assist a person to engage in the conduct of a CHIS, or to obtain information by means of the conduct of a CHIS.

29.3 The conduct of a CHIS is establishing or maintaining a personal or other relationship with another person for the covert purpose of:

a. Using such a relationship to obtain information, or to provide access to information to another person, or

b. Disclosing information obtained by the use of such a relationship or as a consequence of such a relationship or

c. Is incidental to anything falling within a. and b. above.

29.4 In other words, an authorisation for conduct will authorise steps taken by the CHIS on behalf, or at the request, of a public authority.

29.5 The use of a source is what the public authority does in connection with the source, such as the interaction with them to select them and induce them. It will also include what you ask them to do (see section 32). The conduct is what a source does to fulfil whatever tasks are given to them or which is incidental to it. The use and conduct require separate consideration before authorisation. However, they are normally authorised within the same authorisation.

29.6 The same authorisation form is used for both use and conduct. A Handler and Controller must also be designated, as part of the authorisation process, and the application can only be authorised if necessary and proportionate. Detailed records of the use, conduct and tasking of the source also have to be maintained (see section 36).

29.7 Care should be taken to ensure that the CHIS is clear on what is or is not authorised at any given time, and that all the CHIS's activities are properly risk assessed and that risk assessment is properly documented and retained for 5 years after the end of the CHIS authorisation period. If external specialist investigators or investigators employed by a private detective agency are employed by the Council to undertake the CHIS investigation, advice should be taken from them as to the proper content of such risk assessment. Care should also be taken to ensure that relevant applications, reviews, renewals and cancellations are correctly performed, documented and retained in the same way. (Section 2 CHIS Codes of Practice)

29.8 Careful consideration must be given to any particular sensitivities in the local community where the CHIS is being used and of similar activities being undertaken by other public authorities which could have an impact on the deployment of the CHIS. Consideration should also be given to any adverse impact on community confidence or safety that may result from the use or conduct of a CHIS or use of information obtained from that CHIS. (Section 3.27 CHIS Codes of Practice)

Criminal Conduct by a CHIS

29.9 The Covert Human Intelligence Sources (Criminal Conduct) Act 2021 was enacted on 1st March 2021 and it amended RIPA so that **'criminal conduct** in the course of, or otherwise in connection with, the conduct of covert human intelligence sources' is now included in the list of activities capable of being authorised under RIPA as well as Directed and Intrusive surveillance and the use and conduct of a CHIS described above.

29.10 It provides an explicit statutory power for the intelligence agencies, law enforcement and a limited number of wider public authorities, to authorise CHIS to participate in criminal conduct where it is necessary and proportionate to do so. The CHIS Code of Practice contains a section on this and contains the detail required should that be necessary and proportionate.

29.11 So if it is, or becomes necessary to allow a CHIS to commit or assist in what would be regarded as a crime in order to obtain information or evidence of a criminal enterprise then a further authorisation must be obtained and this may occur during the authorisation period of an existing CHIS authorisation which does not cover criminal conduct. Essentially therefore there are now two types of CHIS authorisation one for use and conduct, under s29 of RIPA and one for criminal conduct under section 29 A RIPA. The CHIS Code Section 2 says, '*All criminal conduct that it is envisaged may form part of the conduct of a CHIS should be authorised by means of a separate but linked Section 29B Criminal Conduct Authorisation'.*

30. Handler and Controller

30.1 Covert Human Intelligence Sources may only be authorised if the following arrangements are in place:

- That there will at all times be an officer (the **Handler**) within the Council who will have day to day responsibility for dealing with the source on behalf of the authority, and for the source's security. The Handler is likely to be the investigating officer.

- That there will at all times be another officer within the Council who will have general oversight of the use made of the source; **(Controller)** i.e. the line manager.

- That there will at all times be an officer within the Council who has responsibility for maintaining a record of the use made of the source. See CHIS record keeping (see section 36)

30.2 The **Handler** will have day to day responsibility for:

- Dealing with the source on behalf of the Council;

- Risk assessments

- Directing the day to day activities of the source;
- Recording the information supplied by the source; and
- Monitoring the source's security and welfare.
- Informing the Controller of concerns about the personal circumstances of the CHIS that might effect the validity of the risk assessment or conduct of the CHIS

30.3 The **Controller** will be responsible for:

- The management and supervision of the "Handler" and
- General oversight of the use of the CHIS; (including ensuring that the handler has completed the necessary risk assessments)
- maintaining an audit of case work sufficient to ensure that the use or conduct of the CHIS remains within the parameters of the extant authorisation.

31. Undercover Officers

31.1 Oversight and management arrangements for **undercover operatives**, while following the principles of RIPA, will differ, in order to reflect the specific role of such individuals as officers employed by the Council. The role of the handler will be undertaken by a person such as the investigating officer who in this context may also be referred to as a **'cover officer'** and the role of controller will be undertaken by their line manager who may also be referred to as the **'covert operations manager'**. (Section 7 CHIS Codes of Practice).

32. Tasking

32.1 Tasking is the assignment given to the source by the Handler or Controller such as by asking them to obtain information, to provide access to information or to otherwise act, incidentally, for the benefit of the Council. Authorisation for the use or conduct of a source is required prior to any tasking where the assignment requires the source to establish or maintain a personal or other relationship for a covert purpose.

32.2 In some instances, the tasking given to a person will not require the source to establish a personal or other relationship for a covert purpose. For example, a member of the public is asked to maintain a record of all vehicles arriving and leaving a specific location or to record the details of visitors to a neighbouring house. A relationship has not been established or maintained in order to gather the information and a CHIS authorisation is therefore not available. Other authorisations under RIPA, for example, Directed Surveillance, may need to be considered where there is a possible interference with the Article 8 rights of an individual.

32.3 Authorisations should not be drawn so narrowly that a separate authorisation is required each time the CHIS is tasked. Rather, an authorisation might cover, in broad terms, the nature of the source's task.

32.4 When unforeseen action or undertakings occur on the "use and conduct" of a CHIS whereby it is evident that the CHIS is required to commit, take part in or assist with the commission of a criminal offence or offences a full record must be made, a further risk assessment carried out and a proper assessment must be done to see whether a new authorisation is required.

33. Risk Assessments

33.1 The Council has a responsibility for the safety and welfare of the source and for the consequences to others of any tasks given to the source. It is a requirement of the codes that a risk assessment is carried out. This should be submitted with the authorisation request. The risk assessment should provide details of how the CHIS is going to be handled It should also take into account the safety and welfare of the CHIS in relation to the activity and should consider the likely consequences should the role of the CHIS become known. The ongoing security and welfare of the CHIS after the cancellation of the authorisation should also be considered at the outset.

34. Use of Equipment by a CHIS

34.1 If a CHIS is required to wear or carry a surveillance device such as a covert camera it does not need a separate intrusive or directed surveillance authorisation, provided the device will only be used in the presence of the CHIS. It should be authorised as part of the conduct of the CHIS.

34.2 CHIS, whether or not wearing or carrying a surveillance device, in residential premises or a private vehicle, does not require additional authorisation to record any activity taking place inside those premises or that vehicle which takes place in their presence. This also applies to the recording of telephone conversations. This should have been identified at the planning stage.

35. CHIS Management

35.1 The operation will require managing by the handler and controller which will include ensuring that the activities of the source and the operation remain focused and there is no status drift. It is important that the intrusion is assessed to ensure the operation remains proportionate. The security and welfare of the source will also be monitored. The authorising officer should maintain general oversight of these functions.

35.2 During CHIS activity, there may be occasions when unforeseen actions or undertakings occur. Such incidences should be recorded as soon as practicable after the event and if the existing authorisation is insufficient, it should either be dealt with by way of a review and re-authorised (for minor amendments only) or it should be cancelled, and a new authorisation obtained before any further action is carried out. Similarly, where it is intended to task a CHIS in a new significantly different way than previously identified, the proposed tasking should be referred to the Authorising Officer, who should consider whether a separate authorisation is required. This should be done in advance of any tasking and details of such referrals must be recorded.

36. CHIS Record Keeping

36.1 Central Record of Authorisations

36.2 A centrally retrievable record of all authorisations is held by the Council. This record contains the relevant information to comply with the Codes of Practice. These records are updated whenever an authorisation is granted, renewed or cancelled and are available to the Investigatory Powers Commissioner (IPCO) upon request. (see also paragraphs 55 and 56 of this procedure)

36.3 The records are retained for no less than 5 years from the ending of the authorisation subject to any reasonable increase of this time period in relation to particular cases by the Authorising Officer. (see paragraph 59.6 relating to data protection)

36.4 Individual Source Records of Authorisation and Use of CHIS

36.5 Detailed records must be kept of the authorisation and the use made of a CHIS. An authorising officer must not grant an authorisation for the use or conduct of a CHIS unless they believe 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. The Regulation of Investigatory Powers (Source Records) Regulations 2000; SI No: 2725 details the particulars that must be included in these records.

36.6 The particulars to be contained within the records are;

a. The identity of the source;

b. An identity, where known, used by the source;

c. Any relevant investigating authority other than the authority maintaining the records;

d. The means by which the source is referred to within each relevant investigating authority;

e. Any other significant information connected with the security and welfare of the source;

f. Any confirmation made by a person granting or renewing an authorisation for the conduct or use of a source that the information in paragraph (d) has been considered and that any identified risks to the security and welfare of the source have where appropriate been properly explained to and understood by the source;

g. The date when, and the circumstances in which the source was recruited;

h. Identity of the handler and controller (and details of any changes)

i. The periods during which those persons have discharged those responsibilities;

j. The tasks given to the source and the demands made of him in relation to his activities as a source;

k. All contacts or communications between the source and a person acting on behalf of any relevant investigating authority;

l. The information obtained by each relevant investigating authority by the conduct or use of the source;

m. Any dissemination by that authority of information obtained in that way; and

n. In the case of a source who is not an undercover operative, every payment, benefit or reward and every offer of a payment, benefit or reward that is made or provided by or on behalf of any relevant investigating authority in respect of the source's activities for the benefit of that or any other relevant investigating authority.

36.7 The person maintaining these records are the CHIS Handler and Controller who will pass them on to the RIPA Co-ordinator on a regular basis.

36.8 Public authorities are also encouraged to maintain auditable records for those individuals who are known to provide intelligence on a regular basis but who do not actually meet the definition of a CHIS. This will assist authorities to monitor the status of a human source and identify whether that person should be duly authorised as a CHIS. This should be updated regularly to explain why authorisation is not considered necessary. Such decisions should be made by Authorising Officers. (Section 8 CHIS Codes of Practice).

36.9. Further Documentation

36.10 In addition to the above appropriate records or copies of the following are also retained by the Council:

- A copy of the authorisation together with any supplementary documentation and notification of the approval given by the authorising officer;

- A copy of any renewal of an authorisation, together with the supporting documentation submitted when the renewal was requested;
- The reason why the person renewing an authorisation considered it necessary to do so;
- Any authorisation which was granted or renewed orally (in an urgent case) and the reason why the case was considered urgent;
- Any risk assessment made in relation to the CHIS;
- The circumstances in which tasks were given to the CHIS;
- The value of the CHIS to the investigating authority;
- A record of the results of any reviews of the authorisation;
- The reasons, if any, for not renewing an authorisation;
- The reasons for cancelling an authorisation; and
- The date and time when any instruction was given by the authorising officer that the conduct or use of a CHIS must cease.
- A copy of the decision by a Judicial Commissioner on the renewal of an authorisation beyond 12 months (where applicable).

36.11 The records kept by the Council should be maintained in such a way as to preserve the confidentiality, or prevent disclosure of the identity of the CHIS, and the information provided by that CHIS. (Sec 8 CHIS Codes of Practice)

36.12 Please refer to paragraph 45 below for the relevant application forms which are available from the RIPA Co-Ordinator. They are also available from the Home Office on the www.gov.uk website BUT they will need amending to suit local authority use. The current link to the Home Office forms is below:
https://www.gov.uk/government/collections/ripa-forms--2

PART D. RIPA Roles and Responsibilities

37. The Senior Responsible Officer (SRO)

37.1 The nominated Senior Responsible Officer is the Director of Digital and Business Change (see Appendix B) The SRO with responsibilities for:

- The integrity of the process in place within Blackburn with Darwen Borough Council to authorise directed surveillance and CHIS as well as appropriate arrangements if such investigatory methods are necessary outside of RIPA – (non-RIPA) ;

- Compliance with the relevant sections of RIPA and the Codes of Practice;

- Oversight of the reporting of errors to the Investigatory Powers Commissioner (IPC) 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 Office (IPCO) and the inspectors who support the Commissioner when they conduct their inspections;

- Where necessary, overseeing the implementation of any recommended post-inspection action plans and

- Ensuring that all Authorising Officers are of an appropriate standard, addressing any recommendations and concerns in the inspection reports prepared by the Investigatory Powers Commissioner.

38. RIPA Co-Ordinator

38.1 The RIPA Co-Ordinator who is currently a Principal Solicitor employed by the Council (see appendix B) is responsible for storing all the original authorisations, reviews, renewals and cancellation forms and the signed approval or refusal documentation from the Justice of the Peace. This will include any authorisations that have not been authorised by the Authorising Officer or refused by a Justice of the Peace or Non-RIPA authorisations.

38.2 The RIPA Co-ordinator will: -

- Keep the copies of the forms for a period of at least 5 years from the ending of each authorisation subject to any reasonable increase of this time period in relation to particular cases by the Authorising Officer, (see paragraph 59.6 relating to data protection)

- Keep the Central Record (a requirement of the Codes of Practice) as required in this Guidance of all of the authorisations, renewals and cancellations; and Issue the unique reference number.

- Keep a database for identifying and monitoring expiry dates and renewal dates.

- Along with, Directors, Service Managers, Authorising Officers, and the Investigating Officers must ensure that any electronic and paper records relating to a RIPA investigation are used, retained or destroyed in line with this Guidance, the Councils Information Management policies, departmental retention schedules and the General Data Protection Regulation (GDPR) and Data Protection Act 2018. (DPA)

- Provide administrative support and guidance on the processes involved.

- Monitor the authorisations, renewals and cancellations with a view to ensuring consistency throughout the Council;

- Monitor each department's compliance and act on any cases of non-compliance;

- Organise the provision of training, further guidance and awareness of RIPA and HRA 1998 including the dissemination of the provisions of this Guidance; and review the contents of this Guidance

39. Line Managers Responsibility

Only those Line Managers that are running a team of investigating officers operationally are expected to be fully trained and to follow this Procedure and Guidance.

40. Investigating Officers/Applicant

40.1 The applicant is normally an investigating officer who completes the application section of the RIPA form. Investigating Officers should think about the need to undertake Directed Surveillance or the use of a CHIS before they seek authorisation and, if necessary, discuss it with their Line Manager. Investigating Officers should consider whether they can obtain the information or achieve their objective by using techniques other than covert surveillance.

40.2 The applicant/investigating officer should also communicate with the authorising officer prior to making a RIPA application to resolve any perceived issues prior to the application form being completed.

40.3 The applicant is likely to attend the magistrates' court to seek the approval of a Justice of the Peace (Magistrate) and if approved and involved in the covert activity they must only carry out what is authorised and approved. They will also be responsible for the submission of any reviews, renewals and cancellations.

41. Authorising Officers

41.1 The Regulation of Investigatory Powers (Directed Surveillance and Covert Human Intelligence Sources) Order 2010 prescribes that for Local Authorities the Authorising Officer shall be a Director, Head of Service, Service Manager or equivalent as distinct from the officer responsible for the conduct of an investigation.

41.2 Appendix B lists the Authorising Officers within the Council who can grant authorisations all of which are at the required level.

41.3 The role of the Authorising Officers is to consider whether to authorise, review, or renew an authorisation. They must also officially cancel the RIPA covert activity. Authorising Officers must have been trained to an appropriate level so as to have an understanding of the requirements in the Codes of Practice and that must be satisfied before an authorisation can be granted.

41.4 Authorising Officers should not be responsible for authorising investigations or operations in which they are directly involved. Where an Authorising Officer authorises such an investigation or operation, the Central Record of authorisations should highlight this, and it should be brought to the attention of a Commissioner or Inspector during their next inspection.

41.5 Authorisations must be given in writing by the Authorising Officer by completing the relevant section on the authorisation form. When completing an authorisation, the case should be presented in a fair and balanced way. In particular, all reasonable efforts should be made to take into account information which weakens the case for the authorisation.

41.6 Authorising Officers must explain why they believe the activity is both necessary (see section 42) and proportionate (see section 43), having regard to the collateral intrusion. They must also consider any similar activity which may be taking place, or sensitivities in the area.

41.7 They also need to explain the parameters of the authorisation. (i.e. ‘who, what, how, why, when, where’?) In other words, identify the subject of the operation and who is undertaking it, why it is necessary, in what circumstances and how it is being carried out, the location and the level of the surveillance that is needed to achieve the objective. It is important that this is made clear on the face of the authorisation form as the surveillance operatives are only allowed to carry out what is authorised. This will assist with avoiding errors.

41.8 If any equipment such as covert cameras are to be used, the Authorising Officer should know the capability of the equipment before authorising its use. This will have an impact on collateral intrusion, necessity and proportionality. They should not rubber-stamp a request. It is important that they consider all the facts to justify their decision.

41.9 The Authorising Officer may be required to attend court to explain what has been authorised and why.

41.10 Authorised Officers must read this Guidance and also the relevant RIPA Codes of Practice issued by the Home Office upon which it is based plus current Procedures and any other relevant guidance issued by the IPCO. It is recommended that Authorising Officers can have access to this Guidance on the Council’s intranet so as

to ensure they have the latest version or alternatively obtain a current one from the RIPA Co-Ordinator.

42 Necessity – Legal and Practical

42.1 Obtaining an authorisation under RIPA and for NON-RIPA will only ensure that there is a justifiable interference with an individual's Article 8 rights if it is necessary and proportionate for these activities to take place.

42.2 The first requirement is that there should be a 'legal necessity' i.e. that which is set out in law namely that the person granting an authorisation believe that the authorisation is necessary for one or more of the statutory grounds. For the local authority Directed Surveillance must be shown to be necessary for the prevention and detection of crime and that the crime attracts a custodial sentence of a maximum of 6 months or more, or for the purpose of preventing or detecting specified criminal offences relating to the underage sale of alcohol and tobacco.

42.3 The lawful criteria for CHIS is prevention and detection of crime and prevention of disorder and the offence does not have to have a sentence of 6 months imprisonment.

42.4 'Practical necessity': the applicant and Authorising Officers must also be able to demonstrate why it is necessary in a practical sense. In other words they must ask themselves whether it is necessary to carry out the covert activity to achieve the objectives in all the circumstances of the particular case at hand. This includes assessing whether or not there are any other means of obtaining the same information by a less intrusive method. This is a specific section in the authorisation form.

43. Proportionality

43.1 If the activities are deemed necessary, the Authorising Officer must also be satisfied that they are proportionate to what is 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.

43.2 The authorisation will not be proportionate if it is excessive in the overall circumstances of the case. Each action authorised should be calculated to have a real benefit the investigation or operation and should not be disproportionate or arbitrary. The fact that a suspected offence may be serious will not alone render the proposed 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.

43.3 When explaining proportionality, the Authorising Officer should explain in the authorisation why the methods and tactics to be adopted during the surveillance are proportionate.

43.4 The codes provide guidance relating to proportionality which should be considered by both applicants and Authorising Officers:

- 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.

44. Collateral Intrusion

44.1 Before authorising applications for Directed Surveillance, the Authorising Officer should also take into account the risk of obtaining collateral intrusion which is private information about persons who are not subjects of the surveillance.

44.2 Staff should take measures, wherever practicable, to avoid or minimise unnecessary intrusion into the privacy of those who are not the intended subjects of the surveillance. Where such collateral intrusion is unavoidable, the activities may still be authorised, provided this intrusion is considered proportionate to what is sought to be achieved. The same proportionality tests apply to anticipated collateral intrusion as to intrusion into the privacy of the intended subject of the surveillance.

44.3 All applications must therefore include an assessment of the risk of collateral intrusion and detail the measures taken to limit this to enable the Authorising Officer fully to consider the proportionality of the proposed actions. This is detailed in a section within the authorisation form.

44.4 In order to give proper consideration to collateral intrusion, an Authorising Officer should be given full information regarding the potential scope of the anticipated surveillance, including the likelihood that any equipment deployed may cause intrusion on persons or property other than the subject(s) of the application. If an automated system such as an online search engine is used to obtain the information, the Authorising Officer should be made aware of its potential extent and limitations. Material which is not necessary or proportionate to the aims of the operation or investigation should be discarded or securely retained separately where it may be

required for future evidential purposes. If it is relevant to the investigation it will need to be retained under CPIA. The Authorising Officer should ensure appropriate safeguards for the handling, retention or destruction of such material, as well as compliance with Data Protection Act requirements.

44.5 Where it is proposed to conduct surveillance activity specifically against individuals who are not suspected of direct or culpable involvement in the overall matter being investigated, interference with the privacy of such individuals should not be considered as collateral intrusion but rather as intended intrusion.

44.6 In the event that authorised surveillance unexpectedly and unintentionally interferes with the privacy of any individual other than the intended subject, the authorising officer should be informed by submitting a review form. Consideration should be given in any such case to the need for any separate or additional authorisation.

44.7 If the Council intends to access a social media or other online account to which they have been given access with the consent of the owner, the authority will still need to consider whether the account(s) may contain information about others who have not given their consent. If there is a likelihood of obtaining private information about others, the need for a Directed Surveillance authorisation should be considered, particularly (though not exclusively) where it is intended to monitor the account going forward.

PART E. The Application and Authorisation Process

45. Relevant Forms

45.1 All the forms can be obtained from the RIPA Co-ordinator or Government Website at

https://www.gov.uk/government/collections/ripa-forms--2

NB if you use the ones from the website you must ensure that you adapt them as instructed.

45.2 For Directed Surveillance there are 4 forms within the process.

(NB YOU MUST FIRST ADAPT EACH FORM SO THAT THERE IS ONLY ONE CRITERION IN THE LIST AT PARAGRAPH 6 I.E. FOR THE PURPOSE OF PREVENTING OR DETECTING CRIME OR OF PREVENTING DISORDER AND NOTE THERE IS NO POWER TO APPLY FOR AN URGENT AUTHORISATION SO THAT SHOULD BE DELETED. IF IN DOUBT PLEASE CONTACT THE AUTHORISING OFFICER OR THE RIPA CO-ORDINATOR WHO WILL SUPPLY YOU WITH A CORRECT FORM ACCORDINGLY.)

The links to the forms are:

- Authorisation - https://www.gov.uk/government/publications/application-for-use-of-directed-surveillance
- Review - https://www.gov.uk/government/publications/review-of-use-of-directed-surveillance
- Renewal - https://www.gov.uk/government/publications/renewal-form-for-directed-surveillance
- Cancellation - https://www.gov.uk/government/publications/cancellation-of-use-of-directed-surveillance-form

45.3 For both CHIS authorisations there are 4 forms within the process. They are:

- Authorisation - https://www.gov.uk/government/publications/application-for-the-use-of-covert-human-intelligence-sources-chis
- Review - https://www.gov.uk/government/publications/reviewing-the-use-of-covert-human-intelligence-sources-chis
- Renewal - https://www.gov.uk/government/publications/renewal-of-authorisation-to-use-covert-human-intelligence-sources
- Cancellation - https://www.gov.uk/government/publications/cancellation-of-covert-human-intelligence-sources-chis

45. 4 For Non-RIPA please obtain them from the RIPA Co-ordinator or the above same forms may be adapted and used with an addition in **BOLD** of the words "**'NON-RIPA**" at the head of each page.

NB NON-RIPA FORMS MUST BE ADAPTED AS FOLLOWS: ADD THE WORDS NON-RIPA IN BOLD AT THE TOP OF THE FORM – THESE HAVE BEEN ADAPTED BY THE RIPA CO-ORDINATOR AND WILL BE SUPPLIED ON REQUEST.

46. Duration of Authorisations

46.1 Authorisations must be given for the maximum duration from the date approved by the Justice of the Peace/magistrate (magistrate) but reviewed on a regular basis and formally cancelled when no longer needed. They do not expire, they must be cancelled when the surveillance is no longer proportionate or necessary. Therefore, a Directed Surveillance authorisation will cease to have effect after three months from the date of approval by the magistrate unless renewed or cancelled. Durations detailed below:

Directed Surveillance	3 Months
Renewal	3 Months

Covert Human Intelligence Source	12 Months
Renewal	12 months
Juvenile Sources	4 Months
Renewal	4 Months

46.2 It is the responsibility of the Investigating Officer to make sure that the authorisation is still valid when they undertake surveillance. It is sometimes helpful to think of the authorisation as something like an insurance policy.

47. Applications/Authorisation

47.1 The applicant/investigating officer should take into account the level of intrusion ie the chances of obtaining private information prior to making the application and should communicate with the authorising officer in advance with any concerns prior to applying. The person seeking the authorisation must then complete the application form having regard to, this Guidance and the statutory Codes of Practice. The form should then be submitted to the Authorising Officer for authorisation.

47.2 When completing an application for authorisation, the applicant must ensure that the case for the authorisation is presented in the application in a fair and balanced way. In particular, all reasonable efforts should be made to take into account information which weakens the case for the warrant or authorisation. This is a requirement of the Home Office Codes.

47.3 All the relevant sections must be completed with sufficient information to ensure that applications are sufficiently detailed for the Authorising Officer to consider Necessity, Proportionality having taken into account the Collateral Intrusion issues **Cutting and pasting or using template entries should not take place as this would leave the process open to challenge.**

47.4 If it is intended to undertake both Directed Surveillance and the use of a CHIS on the same surveillance subject, the respective authorisation should be completed and the respective procedures followed. Both activities should be considered separately on their own merits.

47.5 All application forms should be submitted to the Authorising Officer after any internal management requirements have been complied with such as a requirement for Line Manager approval.

47.6 Applications whether authorised or refused will be issued with a unique number (obtained from the RIPA Co-Ordinator) by the Authorising Officer. The number will be taken from the next available number in the Central Record of authorisations which is held by the RIPA Coordinator.

47.7 If not authorised, feedback will be provided to the applicant and the application will be forwarded to the RIPA Co-Ordinator for recording and filing. If having received the

feedback, the applicant feels it is appropriate to re submit the application, they can do so and it will then be considered again.

47.8 Following authorisation, the applicant will then complete the relevant section of the judicial application/order form available on line by accessing the link after the next paragraph. Although this form requires the applicant to provide a brief summary of the circumstances of the case, this is supplementary to and does not replace the need to supply a copy and the original RIPA authorisation as well.

47.9 Government guidance on how to obtain approval from the Justice of the Peace/ magistrates – ie the 'judicial approval' is available on www.gov.uk and access to that guidance and the application form that should be used to submit to the magistrates court can be obtained via the link below. Advice on this can also be obtained from the RIPA Co-Ordinator.

https://www.gov.uk/government/publications/changes-to-local-authority-use-of-ripa

48. Arranging the Court Hearing For Judicial Approval

48.1 It will be necessary within office hours to contact the administration office at the nearest Magistrates' Court to arrange a hearing. The hearing of the application will be in private and on oath before a single Justice of the Peace/magistrate (magistrate).

48.2 Officers who may present the application at these proceedings must ensure they have the requisite delegated powers given by the Council under section 223 of the Local Government Act 1972 to appear, be sworn in and present evidence or information as required by the magistrate. Investigating and Authorising officers who require legal representation for the application may seek advice from the RIPA Co-Ordinator[1].

49. Attending the Hearing

49.1 The Government 2002 Judicial Approval Guidance (see link at 47.9 above) envisages that only the applicant/investigating officer will attend the hearing; however, the IPCO recommends, and it is much better practice for the Authorising Officer also to attend the hearing. This is because the applicant/investigating officer cannot answer questions about the Authorising Officer's own assessment of necessity and proportionality which are key issues about which the court will ask questions. Upon attending the hearing, the officer must present to the court the partially completed judicial application/order form, the original and a copy of the RIPA application/authorisation form, together with any supporting documents setting out the case. The original RIPA authorisation should be shown to the court but will be retained

[1] See Judicial Approval Guidance https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/118173/local-authority-england-wales.pdf

by the Council so that it is available for inspection by IPCO, and in the event of any legal challenge or investigations by the Investigatory Powers Tribunal (IPT).

49.2 The magistrate will read and consider the RIPA authorisation and the judicial application/order form – accessible via the link at paragraph 47.9 above. The magistrate may have questions to clarify points or require additional reassurance on particular matters. These questions are supplementary to the content of the application form**. However, the forms and supporting papers must by themselves make the case. It is not sufficient for the Council to provide oral evidence where this is not reflected or supported in the papers provided**.

49.3 The magistrate will consider whether they are satisfied that, at the time the authorisation was granted or renewed, there were reasonable grounds for believing that the authorisation was necessary and proportionate. In addition, they must be satisfied that the person who granted the authorisation was an appropriate Designated Person within the Council to authorise the activity and the authorisation was made in accordance with any applicable legal restrictions, for example, the crime threshold for Directed Surveillance. (NB The Regulation of Investigatory Powers (Directed Surveillance and Covert Human Intelligence Sources) Order 2010 prescribes that for Local Authorities the Authorising Officer shall be a Director, Head of Service, Service Manager or equivalent as distinct from the officer responsible for the conduct of an investigation. CF Para 41.1 above)

50. Decision of the Magistrate/Justice of the Peace (magistrate)

50.1 The magistrate has a number of options which are:

50.2 **Approve or renew an authorisation.** If approved by the magistrate, the date of the approval becomes the commencement date for the duration of the three months and the officers are now allowed to undertake the activity for that duration.

50.3 **Refuse to approve or renew an authorisation.** The RIPA authorisation will not take effect and the Council may **not** use the technique in that case.

50.4 Where an application has been refused, the applicant may wish to consider the reasons for that refusal. If more information was required by the magistrate to determine whether the authorisation has met the tests, and this is the reason for refusal, the officer should consider whether they can reapply. For example, if there was information to support the application which was available to the Council, but not included in the papers provided at the hearing.

50.5 For, a technical error (which does not alter the substance of the matter or otherwise as may be defined by the magistrate), the form may be remedied without going through the internal authorisation process again. The officer may then wish to reapply for judicial approval once those steps have been taken.

50.6 **Refuse to approve or renew and quash the authorisation.** This applies where the magistrate refuses to approve or renew the authorisation and decides to quash the original authorisation. However, the court must not exercise its power to quash the

authorisation unless the applicant has had at least 2 business days from the date of the refusal in which to make representations. If this is the case, the officer may take advice from the RIPA Co-ordinator or other solicitor employed by the Council who will consider whether to make any representations.

50.7 The magistrate will record the decision on the order section of the judicial application/order form. The court administration will retain a copy of the Council's RIPA application and authorisation form and the judicial application/order form. The officer will retain the original authorisation and a copy of the judicial application/order form.

50.8 The Council may only appeal a magistrates' decision on a point of law by judicial review. If such a concern arises, Legal will decide what action if any should be taken.

50.9 There is a Home Office chart showing the above procedure attached to the Government Guidance referred to and accessible via the link at paragraph 47.9 above

51. Post Court Procedure

51.1 It will be necessary to work out the cancellation date from the date of approval and ensure that the applicant and the Authorising Officer is aware. The original application and the copy of the judicial application/order form should be forwarded to the RIPA Co-Ordinator. A copy will be retained by the applicant and if necessary by the Authorising Officer. The Central Record will be updated with the relevant information to comply with the Codes of Practice and the original documents filed and stored securely.

51.2 Where dates are set within the process such as reviews, they must be adhered to. This will help with demonstrating that the process has been managed correctly in line with the Codes of Practice and reduce the risk of errors.

52. Reviews

52.1 When an application has been authorised and approved by a magistrate, regular reviews must be undertaken by the Authorising Officer to assess the need for the surveillance to continue.

52.2 In each case the Authorising Officer should determine how often a review should take place at the outset. This should be as frequently as is considered necessary and practicable. Particular attention is drawn to the need to review authorisations frequently where the surveillance provides a high level of intrusion into private life or significant collateral intrusion, or confidential information (as defined in para 13). They will record when they are to take place on the application form. This decision will be based on the circumstances of each application. However, reviews will be conducted on a monthly or less basis to ensure that the activity is managed. It will be important for the

Authorising Officer to be aware of when reviews are required to ensure that the applicants submit the review form on time.

52.3 Applicants should submit a review form (to obtain an application form see paragraph 45) by the review date set by the Authorising Officer. They should also use a review form for changes in circumstances to the original application which would include a change to the level of intrusion so that the need to continue the activity can be re-assessed. However, if the circumstances or the objectives have changed considerably, or the techniques to be used are now different, a new application form should be submitted, and it will be necessary to follow the process again and be approved by a magistrate. The applicant does not have to wait until the review date if it is being submitted for a change in circumstances.

52.4 Line mangers of applicants may need to make themselves aware of when the reviews are required in accordance with internal staff management arrangements to ensure that the relevant forms are completed on time.

52.5 The reviews are dealt with internally by submitting the review form to the Authorising Officer. There is no requirement for a review form to be submitted to a magistrate.

52.6 The results of a review should be recorded on the Central Record.

52.7 NB Reviews should also be undertaken in relation to NON-RIPA cases – all of the above applies also to them except for reference to magistrates' approval.

53. Renewals

53.1 A renewal form is to be completed by the applicant when the original authorisation period is about to expire but Directed Surveillance or the use of a CHIS is still required. (to obtain an application form see paragraph 45)

53.2 Should it be necessary to renew an authorisation for Directed Surveillance or CHIS, this must be approved by a magistrate.

53.3 Applications for renewals should not be made until shortly before the original authorisation period is due to expire. However, they must take account of factors which may delay the renewal process (e.g. intervening weekends or the availability of the relevant Authorising Officer and a magistrate to consider the application).

53.4 The applicant should complete all the sections within the renewal form and submit the form to the Authorising Officer for consideration.

53.5 Authorising Officers should examine the circumstances with regard to Necessity, Proportionality and the Collateral Intrusions issues before making a decision to renew the activity. A CHIS application should not be renewed unless a thorough review has been carried out covering the use made of the source, the tasks given to them and information obtained. The Authorising Officer must consider the results of the review when deciding whether to renew or not. The review and the consideration must be documented.

53.6 If the Authorising Officer refuses to renew the application, the cancellation process should be completed. If the Authorising Officer authorises the renewal of the activity, the same process is to be followed as for the initial application and approval must be sought from a magistrate.

53.7 A renewal takes effect on the day on which the authorisation would have ceased and lasts for a further period of three months.

53.8 Renewal forms should also be used as above in relation to Non-RIPA cases.

54. Cancellation

54.1 The cancellation form must be submitted to the authorising officer by the applicant or another investigator in their absence. (to obtain the forms see paragraph 45) The Authorising Officer who granted or last renewed the authorisation must authorise the cancellation if they are satisfied that the Directed Surveillance no longer meets the criteria upon which it was authorised. Where the Authorising Officer is no longer available, this duty will fall on the person who has taken over the role of Authorising Officer or the person who is acting as Authorising Officer. NB If the directed surveillance of CHIS runs its course to the end of the three months or 12 months – it must not be allowed to simply expire – the completion of a cancellation form is still required.

54.2 As soon as the decision is taken that Directed Surveillance should be discontinued, the applicant or other investigating officer involved in the investigation should inform the Authorising Officer. The Authorising Officer will formally instruct the investigating officer to cease the surveillance, noting the time and date of their decision. This will be required for the cancellation form. The date and time when such an instruction was given should also be recorded in the Central Record of authorisations**.**

54.3 The Investigating Officer submitting the cancellation should complete in detail the relevant sections of the form and include the period of surveillance and detail if any images were obtained, particularly any images containing innocent third parties. The Authorising Officer should then take this into account and issues instructions regarding the management and disposal of the images etc. See sections 58 to 65 Safeguarding and the Use of Surveillance Material below.

54.4 The cancellation process should also be used to evaluate whether the objectives have been achieved and whether the applicant carried out what was authorised. This check will form part of the oversight function. Where issues are identified including errors (see section 65), they will be brought to the attention of the RIPA Co-Ordinator and the Senior Responsible Officer (SRO) (and also the line manager for internal management purposes). This will assist with future audits and oversight and comply with the Codes of Practice.

54.5 When cancelling a CHIS authorisation, an assessment of the welfare and safety of the source should also be assessed, and any issues identified.

54.6 All cancellations must be submitted to the RIPA Co-Ordinator for inclusion in the Central Record and storing securely with the other associated forms.

54.7 Do not wait until the 3 month period is up to cancel. Cancel it at the earliest opportunity when no longer necessary and proportionate. Line Managers should be aware of when the activity needs cancelling and ensure that staff comply with the procedure.

Part F Central Record and Safe-keeping of the Material

55. Introduction

55.1 Authorising Officers, applicants and line managers of relevant enforcement departments may keep whatever records they see fit to administer and manage the RIPA application process. This includes the legal obligations under the Criminal Procedures and Investigations Act 1996. However, this will not replace the requirements under the RIPA Codes of Practice, which includes the fact that the Council must hold a centrally held and retrievable record.

56. Central Record

56.1 The centrally retrievable record of all authorisations will be held and maintained by the RIPA Co-Ordinator. It will be regularly updated whenever an authorisation is applied for, refused, granted, renewed or cancelled. The record will be made available to the relevant Commissioner or an Inspector from IPCO, upon request.

56.2 All original authorisations and copies of Judicial applications/order forms whether authorised or refused, together with review, renewal and cancellation documents, must be sent within 48 hrs to the RIPA Co-Ordinator who will be responsible for maintaining the Central Record of authorisations. They will ensure that all records are held securely with no unauthorised access. If in paper format, they must be forwarded in a sealed envelope marked confidential.

56.3 The documents contained in the Central Record should be retained for at least 5 years from the ending of the authorisation subject to any reasonable increase of this time period in relation to particular cases by the Authorising Officer. (see paragraph 59.6 relating to data protection) The Central Record contains the following information:

- If refused, (the application was not authorised by the AO) a brief explanation of the reason why. The refused application should be retained as part of the Central Record of authorisation;

- If granted, the type of authorisation and the date the authorisation was given;

- Details of attendances at the magistrates' court to include the date of attendances at court, the determining magistrate, the decision of the court and the time and date of that decision;

- Name and rank/grade of the authorising officer;

- The unique reference number (URN) of the investigation or operation;

- The title of the investigation or operation, including a brief description and names of subjects, if known;

- Frequency and the result of each review of the authorisation;

- If the authorisation is renewed, when it was renewed and who authorised the renewal, including the name and rank/grade of the authorising officer and the date renewed by the JP;

- Whether the investigation or operation is likely to result in obtaining confidential information (as defined in para 13);

- The date the authorisation was cancelled;

- Authorisations by an Authorising Officer where they are directly involved in the investigation or operation. If this has taken place it must be brought to the attention of a Commissioner or Inspector during their next RIPA inspection.

56.4 As well as the Central Record the the RIPA Co- ordinator will also retain:

- The original of each application, review, renewal and cancellation, copy of the judicial application/order form, together with any supplementary documentation of the approval given by the Authorising Officer;
- The frequency and result of reviews prescribed by the Authorising Officer;

- The date and time when any instruction to cease surveillance was given;

- The date and time when any other instruction was given by the Authorising Officer;

- A record of the period over which the surveillance has taken place. This should have been included within the cancellation form.

56.5 These documents will also be retained for 5 years from the ending of the authorisation subject to any justifiable increase of this time period in relation to particular cases by the Authorising Officer. (see paragraph 59.6 relating to data protection)

57. Safe-keeping and the Use of Surveillance Material

57.1 This part of the Guidance (part F) provides guidance on the procedures to be applied in relation to the handling of any material obtained through Directed Surveillance or CHIS activity. This material may include private, confidential or legally privileged information. It will also show the link to other relevant legislation.

57.2 The Council should ensure that their actions when handling information obtained by means of covert surveillance or CHIS activity comply with relevant legal frameworks and the Codes of Practice, so that any interference with privacy is justified in accordance with Article 8(2) of the European Convention on Human Rights. Compliance with these legal frameworks, including Data Protection requirements, will ensure that the handling of private information obtained continues to be lawful, justified and strictly controlled, and is subject to robust and effective safeguards. The material will also be subject to the Criminal Procedure and Investigations Act (CPIA) 1996.

58. Authorised Purpose

58.1 Dissemination, copying and retention of material must be limited to the minimum necessary for authorised purposes. For the purposes of the RIPA codes, something is necessary for the authorised purposes if the material:

- Is, or is likely to become, necessary for any of the statutory purposes set out in RIPA in relation to covert surveillance or CHIS activity;
- Is necessary for facilitating the carrying out of the functions of public authorities under RIPA;
- Is necessary for facilitating the carrying out of any functions of the Commissioner or the Investigatory Powers Tribunal;
- Is necessary for the purposes of legal proceedings; or
- Is necessary for the performance of the functions of any person by or under any enactment.

59. Handling and Retention of All Surveillance and Associated Material

59.1 As mentioned above, all material associated and obtained with an application will be subject of the provisions of the Data Protection Act (DPA) 2018, GDPR, Home Office RIPA Codes of Practice (Covert Surveillance and Property Interference and CHIS) and CPIA Codes of Practice. This material includes but is not limited to: e-mails between officers relating to a RIPA application, RIPA application forms pre- and post-authorisation approval, risk assessments, advice sought from managers and authorising officers. Each and every officer involved within this process and copied in to any chain of e-mails about a RIPA application or the product of the application should

make themselves aware of the provisions within this legislation and how it impacts on the whole RIPA process. Authorising Officers are responsible for ensuring that material obtained, together with relevant associated paperwork should be held securely and ensuring that application forms are only held by those who need to see them. No officers other than the investigating officer who made the application and the authorising officers should hold those application forms. After authorisation has been cancelled authorising officers should apply their minds to whether the material needs to be retained bearing in mind that the RIPA Co-ordinator should already have been supplied with all the forms for the Central Record. Extra care needs to be taken if the application and material relates to a CHIS in the sense that there should be restricted access to those who need to see the records, ideally, the handler and controller only, with an option for Senior Managers and /or auditors to request access if necessary. There should also be appropriate security such as password protection and lockable safes.

59.2 Material required to be retained under CPIA should be retained until a decision is taken whether to institute proceedings against a person for an offence or if proceedings have been instituted, at least until the accused is acquitted or convicted or the prosecutor decides not to proceed with the case. The records must be kept by the absolute minimum number of officers. Authorising officers are responsible, upon signing the cancellation form for the surveillance/CHIS, for contacting each officer in the chain of command including the relevant Disclosure Officers and ensuring that they have destroyed the material at the point at which it no longer has any bearing upon the investigation. The material should not be kept for longer than one year unless it can be justified. The Authorising Officer in the case should make a documented decision and justify it with reasons if it is to be kept any longer. In particular, any application forms pre- or post-authorisation or emails to which they are attached do not need to be kept at all if they are not relevant to the investigation. If a copy of an authorisation is needed for audit purposes then a request should be made to the RIPA Co-ordinator to view the authorisation document that is kept in the Central Record. Multiple copies are not required to be kept by any other individuals.

59.3 Where the accused is convicted, all material which may be relevant must be retained at least until the convicted person is released from custody, or six months from the date of conviction, in all other cases.

59.4 If the court imposes a custodial sentence and the convicted person is released from custody earlier than six months from the date of conviction, all material which may be relevant must be retained at least until six months from the date of conviction.

59.5 If an appeal against conviction is in progress when released, or at the end of the period of six months, all material which may be relevant must be retained until the appeal is determined.

59.6 If retention is beyond these periods it must be justified for data protection purposes under the GDPR and or Data Protection Act 2018 (DPA). Each relevant service within the Council may have its own provisions under their Data Retention Guidance which will also need to be consulted to ensure that the data is retained lawfully and for as long as is necessary.

60. Use of Material as Evidence

60.1 Material obtained through Directed Surveillance, may be used as evidence in criminal proceedings. The admissibility of evidence in criminal proceedings or civil proceedings is governed by common law and many pieces of legislation notably including the Police and Criminal Evidence Act 1984, Criminal Procedure and Investigations Act 1996 (CPIA), Criminal Justice Act 2003, Civil Evidence Act 1995 and subordinate legislation such as both the Civil and Criminal Procedure Rules. Also challenges to the way evidence is gathered can be made if it can be shown that there has been a breach of Articles 8 (privacy) and /or 6 (fair trial) of the European Convention as adopted in the Schedule to the Human Rights Act 1998.

60.2 Ensuring the continuity and integrity of evidence is critical to every prosecution. Accordingly, considerations as to evidential integrity are an important part of the disclosure regime under the CPIA and these considerations will apply to any material acquired through covert surveillance that is used in evidence. When information obtained under a covert surveillance authorisation is used evidentially, the Council will be able to demonstrate how the evidence has been obtained, to the extent required by the relevant rules of evidence and disclosure.

60.3 Where the product of surveillance could be relevant to pending or future criminal or civil proceedings, it should be retained in accordance with established disclosure requirements. In a criminal case the codes issued under CPIA will apply. They require that the investigator record and retain all relevant material obtained in an investigation and later disclose relevant material to the Prosecuting Solicitor. They in turn will decide what is disclosed to the Defence Solicitors.

60.4 There is nothing in RIPA which prevents material obtained under Directed Surveillance authorisations from being used to further other investigations

61. Dissemination of Information

61.1 It may be necessary to disseminate material acquired through the RIPA covert activity within the Council or shared outside with other Councils or agencies, including the Police. The number of persons to whom any of the information is disclosed, and the extent of disclosure, should be limited to the minimum necessary. It must also be in connection with an authorised purpose as set out in sec 58 above. It will be necessary to consider exactly what and how much information should be disclosed. Only so much of the material may be disclosed as the recipient needs; for example, if a summary of the material will suffice, no more than that should be disclosed.

61.2 The obligations apply not just to the Council as the original authority acquiring the information, but also to anyone to whom the material is subsequently disclosed. In some cases, this will be achieved by requiring the latter to obtain permission from the Council before disclosing the material further. It is important that the Authorising Officer and line manager in charge of the enquiry considers these implications at the point of dissemination to ensure that safeguards are applied to the data.

61.3 A record will be maintained justifying any dissemination of material. If in doubt, seek advice.

62. Storage

62.1 Material obtained through covert surveillance and CHIS authorisations, and all copies, extracts and summaries of it, must be handled and stored securely, so as to minimise the risk of loss. It must be held so as to be inaccessible to persons who are not required to see the material (where applicable). This requirement to store such material securely applies to all those who are responsible for the handling of the material. It will be necessary to ensure that both physical and IT security and an appropriate security clearance regime is in place to safeguard the material.

63. Copying

63.1 Material obtained through covert surveillance may only be copied to the extent necessary for the authorised purposes set out above. Copies include not only direct copies of the whole of the material, but also extracts and summaries which identify themselves as the product of covert surveillance, and any record which refers to the covert surveillance and the identities of the persons to whom the material relates.

63.2 In the course of an investigation, the Council must not act on or further disseminate legally privileged items unless it has first informed the Investigatory Powers Commissioner that the items have been obtained.

64. Destruction

64.1 Information obtained through covert surveillance, and all copies, extracts and summaries which contain such material, should be scheduled for deletion or destruction and securely destroyed as soon as they are no longer needed for the authorised purpose(s) set out above. If such information is retained, it should be reviewed at appropriate intervals to confirm that the justification for its retention is still valid. In this context, destroying material means taking such steps as might be necessary to make access to the data impossible.

Part G. Errors and Complaints

65. Errors

65.1 Errors can have very significant consequences on an affected individual's rights. Proper application of the surveillance and CHIS provisions in the RIPA codes and this Guidance should reduce the scope for making errors.

65.2. There are two types of errors within the codes of practice which are:

- Relevant error and
- Serious error.

65.3 Relevant Error

65.4 An error must be reported if it is a "**relevant error**". A relevant error is any error in complying with any requirements that are imposed on a public authority by any enactment which are subject to review by a Judicial Commissioner. This would include compliance by public authorities with Part II of the RIPA.

65.5 Examples of relevant errors occurring would include circumstances where:

- Surveillance 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 Chapter 9 of the Surveillance Codes of Practice relating to the safeguards of the material.

65.6 All relevant errors made by the Council (and its employees) must be reported to the Investigatory Powers Commissioner by the Council as soon as reasonably practicable and a full report no later than ten working days. The report should include information on the cause of the error; the amount of surveillance conducted, and material obtained or disclosed; any unintended collateral intrusion; any analysis or action taken; whether any material has been retained or destroyed; and a summary of the steps taken to prevent recurrence.

65.7 Serious Errors

65.8 The Investigatory Powers Commissioner must inform a person of any relevant error relating to that person if the Commissioner considers that the error is a serious error and that it is in the public interest for the person concerned to be informed of the error. The Commissioner may not decide that an error is a serious error unless they consider that the error has caused significant prejudice or harm to the person concerned. The fact that there has been a breach of a person's Convention rights (within the meaning of the Human Rights Act 1998) is not sufficient by itself for an error to be a serious error.

65.9 It is important that all staff involved in the RIPA process report any issues, so they can be assessed as to whether it constitutes an error which requires reporting.

66. Complaints

66.1 Any person who reasonably believes they have been adversely affected by surveillance activity by or on behalf of the Council may complain to the RIPA Co-Ordinator who will investigate the complaint and report the findings to the Senior Responsible Officer. A complaint can also be made to the official body which is the Investigatory Powers Tribunal (IPT). They have jurisdiction to investigate and determine complaints against any public authority's use of RIPA powers, including those covered by this Guidance.

66.2 Complaints should be addressed to:

The Investigatory Powers Tribunal

PO Box 33220

London

SWIH 9ZQ

Change Control

Item	Reason for Change	Version	Author	Date	Council Decsions
Regulation of Investigatory Powers Act 2000 (RIPA) Procedure and Guidance	Completely new version to replace the previous one in line with and referring to the updated Government Codes of Practice	Version 1	Shelagh Lyth Principal Solicitor (Litigation) based on a template provided by specialist and trainer P	2021	Approved by Overview and Scrutiny Committee 20 June 2022 and Executive Board on 14 July 2022

			Fowler and adapted to BwD processes		
As above	Amended to incorporate amendments recommended by the Inspector of the Office of Investigatory Powers Commissioner in November 2022 relating to records retention and security and also to reflect the further changes to the Home Office Codes of Practice	Version 2	Shelagh Lyth Principal Solicitor (Litigation)	2023	Approved by Overview and Scrutiny Committee on 17 July 2023

APPENDIX A

INTERNET & SOCIAL MEDIA RESEARCH & INVESTIGATIONS GUIDANCE

1. Introduction

1.1 Online open source research is widely regarded as the collection, evaluation and analysis of material from online sources available to the public, whether by payment or otherwise to use as intelligence and evidence.

1.2 The use of online open source internet and social media research is a method of obtaining information to assist the Council with its regulatory and enforcement functions. It can also assist with service delivery issues. However, the use of the internet and social media is constantly evolving and with it the risks, particularly regarding breaches of privacy under Article 8 Human Rights Act (HRA) and other operational risks.

1.3 Blackburn with Darwen Council (the Council), as a public authority, is, in law, subject to the Human Rights Act 1998, and as such, the staff of the authority must always work within this legislation. This applies to research on the internet.

1.4 Researching, recording, storing, and using open source information regarding a person or group of people must be both necessary and proportionate and take account of the level of intrusion against any person. The activity may also require authorisation and approval by a magistrate under the Regulation of Investigatory Powers Act (RIPA) 2000 if it is involves Directed Surveillance or acting as a CHIS. To ensure that any resultant interference with a person's Article 8 right to respect for their private and family life is lawful, the material must also be retained and processed in accordance with the principles of the General Data Protection Regulations (GDPR).

2. Scope of this Social Media Research Guidance (Appendix A Guidance)

2.1 This Social Media Research Guidance is Appendix A of the Council's RIPA Procedural Guidance and this and any associated internal operational guidance adopted by managers of officers undertaking investigations establish the Council's approach to ensure that all the online research and investigations are conducted by its officers in such a way that it is lawful and ethical to reduce risk. It provides guidance to all officers employed by the Council of the implications and legislative framework associated with online internet and social media research. It will also ensure that the activity undertaken, and any evidence obtained will stand up to scrutiny.

2.2 This Appendix A Guidance takes account of the Human Rights Act 1998, Regulation of Investigatory Powers Act (RIPA) 2000, Criminal Procedures Investigations Act (CPIA) 1996, General Data Protection Regulations (GDPR), NPCC Guidance on Open Source Investigation/Research.

2.3 This Appendix A Guidance and any associated operational guidance will be followed at all times and should be read where required with the Council's RIPA Procedural Guidance to which it is appended and with the Home Office RIPA Codes of Practice. Should there be any queries, advice can be sought from the RIPA Co-ordinator and/or the Social Media Officer – See Appendix B list of relevant officers.

2.4 As with the RIPA Procedural Guide, members of staff who knowingly fail to adhere to this Appendix A Guidance and associated operational procedures could result in members of staff being dealt with through the Council's disciplinary procedure.

2.5 This Appendix A Guidance should not be exempt from disclosure under the Freedom of Information Act 2000

3. Risk

3.1 Staff must be aware that any activity carried out over the internet leaves a trace or footprint which can identify the device used, and, in some circumstances, the individual carrying out the activity and that there is a risk of a breach of Article 8.

3.2 Article 8 is a European Convention right enshrined in the Human Rights Act 1998 which states "Everyone has the right to respect for his private and family life, his home and his correspondence". 8.2 states "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". The Council must act in a way that is compatible with that Convention right.

3.3 With any breach of this Article 8 Convention right there is also a risk of compromise to an ongoing investigation, therefore, the activity should be conducted in a manner that does not compromise any current or future investigation or tactics.

3.4 It should be standard practice for the staff member to complete a risk assessment prior to and during open source internet and social media research.

4. Necessity / Justification

4.1 To justify the research, there must be a clear lawful reason, and it must be necessary for any of the purposes set out in Article 8 eg prevention of crime or disorder. Therefore, the reason for the research must be identified and clearly described. This should be documented with clear objectives. Should the research be aimed at serious criminal conduct and fall within RIPA activity, a properly constituted RIPA authorisation can render the research 'lawful for all purposes'.

5. Proportionality

5.1 Proportionality involves balancing the intrusiveness of the research on the subject and other innocent third parties who might be affected by it (collateral intrusion) against the need for the activity in operational terms. The Council should question what the benefit of carrying out the activity is and how that benefit will outweigh the intrusion and set out the answers to those questions clearly.

5.2 The activity will not be proportionate if it is excessive in the circumstances of the case or if the information which is sought could reasonably be obtained by other less intrusive means. All such activity should be carefully managed to meet the objective in question and must not be arbitrary or unfair.

6 Private information

6.1 Private information is defined in the RIPA Codes of Practice and states it "includes any information relating to a person's private or family life". Private information should be

taken generally to include any aspect of a person's private or personal relationship with others, including family and professional or business relationships. From a data protection perspective, personal data (information as defined by the UK GDPR as 'any information relating to an identified or identifiable natural person') also falls within this definition[2].

6.2 Prior to, and during any research, staff must take into account the privacy issues regarding any person associated with the research.

6.3 Where it is deemed necessary to undertake an investigation to which RIPA is not applicable because it does not meet the serious criminal offence threshold test or where it is not a criminal investigation per se, then, if the officer is concerned that a private information (which amounts to personal data) a risk assessment should be completed and this should reveal the level of risk and how to mitigate it.

7. Reviewing the Activity

7.1 During the course of conducting the internet open source research, the nature of the online activity may evolve. It is important staff continually assess and review their activity to ensure it remains lawful and compliant. Where it evolves into RIPA activity, the RIPA procedure should be followed. If in doubt, seek advice from the RIPA Co-ordinator or the Social Media Lead Officer.

8. Use of Material

8.1 The material obtained from conducting open source internet and social media research may be used as intelligence or evidence.

8.2 Any material gathered from the internet during the course of a criminal investigation must be retained in compliance with the Criminal Procedure and Investigations Act (CPIA) Codes of Practice and all material stored in line with the General Data Protection Regulations (GDPR) data retention policy

9. Monitoring and Review of Social Media Policy

9.1 This Appendix A Guidance will be monitored and reviewed where necessary by the RIPA Co-ordinator at the same time as the RIPA Procedure and Guidance to which this is an Appendix.

[1] "'personal data' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person".

APPENDIX B

Regulation of Investigatory Powers Act 2000 (RIPA) **Procedure and Guidance**

Appendix B List Relevant Officers names and titles

Authorising Officers

The Chief Executive – Denise Park (Only where the Directed surveillance or use of Chis may result in the obtaining of 'confidential information')

The Head of Public Protection – Gary Johnston

The Head of Audit and Assurance – Colin Ferguson

Other Responsible Officers

RIPA Co-Ordinator – Principal Solicitor– Shelagh Lyth

The Senior Responsible Officer (SRO) – Deputy Director Legal and Governance– Asad Laher

The Social Media Lead Officer – Ben Greenwood.