CUMBERLAND COUNCIL

REGULATION OF INVESTIGATORY POWERS ACT 2000

POLICY AND GUIDANCE NOTICES FOR STAFF RELATING TO SURVEILLANCE AND USE OF COVERT HUMAN INTELLIGENCE SOURCES

IMPORTANT NOTICE

The RIPA regime is subject to oversight by the Investigatory Powers Commissioner's Office. Advice, guidance and Codes of Practice may be found at www.ipco.org.uk

RIPA Codes of Practice and Guidance may be found at www.gov.uk/government/collections/ripa-codes

The Council's RIPA Policy is subordinate to the Codes of Practice.

Internal points of contact are:

Clare Liddle:	RIPA Monitoring Officer
Kate Turner:	Deputy RIPA Monitoring Officer

GENERAL STATEMENT OF POLICY

This policy document explains how Cumberland Council will comply with the Regulation of Investigatory Powers Act 2000 ('RIPA') in relation to directed surveillance, use of covert human intelligence sources and the acquisition of communications data. This Policy is supplementary to the legislation and to the statutory Codes of Practice.

For the purposes of this policy, the following Chief Officers are authorised throughout under the term "Chief Officer":

i) the Chief Executive (Head of Paid Service);
ii) the Director of Adult Social Care and Housing;
iii) the Director of Children and Family Wellbeing;
iv) the Director of Public Health and Communities; and
v) the Director of Resources.

For the purposes of this policy, the following are authorised throughout under the term "Senior Lawyer"

I) the Senior Manager, Legal and Democratic Services
II) any Group Lawyer

1.0 Background

1.1 The primary function of central and local government regulation and enforcement is to protect the individual, the environment, and a variety of groups such as consumers and workers. At the same time, carrying out regulatory functions in an equitable, practical and consistent manner helps to promote a thriving national and local economy, and to prevent and detect crime and disorder.

1.2 The Regulation of Investigatory Powers Act 2000 (RIPA) came into effect in September 2000. RIPA sets out a regulatory framework for this use of covert surveillance techniques by public authorities. RIPA does not provide any powers to carry out covert activities. If such activities are conducted by any of the Council's officers then RIPA regulates them in a manner which is compatible with the European Convention on Human Rights (ECHR), particularly Article 8, the right to respect for private and family life. Before undertaking surveillance under RIPA, the Council must satisfy itself that it is undertaken in connection with a core function.

1.3 Sections 37 and 38 of the Protection of Freedoms Act 2012 (the Act) came into force on 1 November 2012. Under the Act local authority authorisations and notices, for the use of particular covert techniques, can only be given effect once an order approving the authorisation or notice has been granted by a Justice of the Peace (JP).

1.4 In addition amendments to the Regulation of Investigatory Powers (Directed Surveillance and Covert Human Intelligence Sources) Order 2010 ("the 2010 Order") mean that a local authority can now only grant an authorisation under RIPA for the use of directed surveillance where

the local authority is investigating particular types of criminal offences. These are criminal offences which attract a maximum custodial sentence of six months or more or criminal offences relating to the underage sale of alcohol or tobacco.

1.5 Communications data is governed by RIPA and the Investigatory Powers Act 2016 (IPA 2016) and the associated Code of Practice on Communications Data 2018. A request for a RIPA authorisation or notice will be scrutinised by a single point of contact (a 'SPoC'). Local Authorities are not able to intercept communications data. Where communications data is required then responsibility for its acquisition rests with the National Anti-Fraud Network (NAFN) who provide the SPoC service. Cumberland Council has an agreement with NAFN for this service.

1.6 Responsibility for oversight of investigatory powers, including inspection and audit is now with the Investigatory Powers Commissioner (IPC) and no longer rests with the Interception of Communications Commissioner's Office (IOCCO), the Office of Surveillance Commissioners (OSC) and the Intelligence Services Commissioner (ISComm) from September 2017.

1.7 Revised Codes of Practice relating to covert surveillance and property Interference and for the investigation of protected electronic information came into force on 15 August 2018. These reflect changes introduced by the IPA 2016 including the introduction of equipment interference warrants under Part 5 of the IPA 2016 Act and the new oversight framework establishing the Investigatory Powers Commissioner.

1.8 Cumberland Council will on occasion need to consider the use of covert surveillance in order to carry out its enforcement functions effectively. Examples of enforcement activities which may require the use of RIPA include trading standards, environmental health, fraud investigations and housing. Other areas such as the investigation of employees for the purpose of disciplinary proceedings do not fall within the RIPA framework.

1.9 The Council takes seriously its responsibilities as a regulatory authority and will at all times act in accordance with the law, ensuring that any regulatory and enforcement action it takes is lawful, necessary and proportionate.

1.10 **Non-RIPA activities.** RIPA does not apply to investigations which are not part of the Council's core functions and it does not apply where the threshold test is not met, as set out in this policy. This does not however preclude the Council from using tools such as Directed Surveillance in other circumstances, such as in the course of disciplinary investigations. In order to safeguard against abuse, the RIPA principles of necessity, proportionality and collateral intrusion must however still be applied to non-RIPA applications in order to comply with human rights protections. The investigator must apply in the same way, to the Authorising Officer using the same forms marked

"non-RIPA". The flow chart at appendix 2 provides information as to whether RIPA or non-RIPA authorisation is required. Non-RIPA applications must be completed and authorised in accordance with this procedure.

2.0 Scope and Definitions

2.1 This policy applies to all Cumberland Council services.

2.2 The main purpose of RIPA is to ensure that the relevant investigatory powers are used in accordance with human rights. These powers are:

i. Interception of communications
ii. Acquisition of communications data (e.g. billing data)
iii. Intrusive surveillance (on residential premises/in private vehicles)
iv. Directed surveillance in the course of specific operations
v. Use of covert human intelligence sources (informants etc.)
vi. Access to encrypted data

2.3 By working in conjunction with other, pre-existing legislation, the Act ensures the following points are clearly covered:

i. purposes to which relevant powers may be used
ii. which authorities can use the powers
iii. authorisation of the use of the powers
iv. the use that can be made of material gained
v. independent judicial oversight
vi. a means of redress for the individual where powers are breached

2.4 RIPA limits local authorities to using three covert techniques for the purposes of the prevention or detection of crime or prevention of disorder. These techniques are:

i. **Directed surveillance** - surveillance which is covert but not intrusive, and which is undertaken for the purposes of a specific investigation or a specific operation, in such a manner as is likely to result in obtaining information about a person – whether or not the target of the investigation/operation.

ii. A **covert human intelligence source (CHIS) -** undercover officers, public informants and people who make test purchases.

iii. **Communications data** (CD) is the ‘who’, ‘when’ and ‘where’ of a communication, but not the ‘what’ (i.e. the content of what was said or written). RIPA groups CD into 3 parts:

iv. ‘traffic data’ (which includes information about where the communications are made or received);

v. ‘service use information’ (such as the type of communication, time sent and its duration); and
vi. ‘entity data (which includes billing information such as the name, address and bank details of the subscriber of telephone or internet services).

2.5 Under RIPA a local authority can only authorise the acquisition of the less intrusive types of communications data: service use and entity data. Under **no circumstances** can local authorities be authorised to obtain traffic data under RIPA.

2.6 The council must be satisfied that there is an identifiable offence before authorising any covert surveillance. In addition, the key tests in an application for authorisation are:

i. Necessity
ii. Proportionality and
iii. Risk of collateral intrusion

3.0 PART 1 – DIRECTED SURVEILLANCE

3.1 Directed surveillance is defined in Section 26(2) of RIPA as surveillance which is covert, but not intrusive, and undertaken:

i. for the purposes of a specific investigation or specific operation;

ii. in such a manner as it is likely to result in the obtaining of **private information** about the person (whether or not one specifically identified for the purposes of the investigation or operation); and

iii. otherwise than by way of an immediate response to events or circumstances, the nature of which is such that it would not be reasonably practical for an authorisation under Part II of RIPA to be sought for the carrying out of the surveillance

3.2 The council will only use directed surveillance to investigate a crime and where the criminal offence being investigated meets one of the following conditions:

i. The offence is punishable, whether on summary conviction or on indictment to a maximum term of at least 6 months of imprisonment, or

ii. Section 146, 147 or 147A of the Licensing Act 2003 (sale of alcohol to children) or

iii. Section 7 of the Children’s and Young Persons Act 1933 (sale of tobacco to children)

3.3 The crime threshold applies only to the authorisation of **directed surveillance** by local authorities under RIPA, not to the authorisation of local authority use of CHIS or their acquisition of CD.

3.4 No officer of the council will undertake intrusive surveillance. Intrusive surveillance is covert surveillance that is carried out in relation to anything taking place on residential premises or in any private vehicle and which involves the presence of an individual on the premises or in the vehicle or is carried out by means of a surveillance device.

3.5 Surveillance operations will only be carried out by officers who have received appropriate training in human rights and the Act.

3.6 No officer within the Council will undertake directed surveillance without prior authorisation.

3.7 Authorisation will only be given by the Chief Officer.

3.8 The use of directed surveillance under RIPA will not be authorised to investigate matters that do not involve criminal offences or to investigate low-level offences that do not meet the threshold test.

4.0 PART 2 - COVERT HUMAN INTELLIGENCE SOURCE (CHIS)

4.1 A covert human intelligence source (CHIS") is defined by section 26(8) of RIPA as a person who:

i. establishes or maintains a personal or other relationship with another person for the covert purpose of facilitating the doing of anything falling within the following two paragraphs;

ii. covertly uses such a relationship to obtain information or to provide access to any information to another person: or

iii. covertly discloses information obtained by the use of such a relationship or as a consequence of the existence of such a relationship

4.2 The authorisation for the conduct and use of a CHIS may include:

i. someone employed or engaged by the Council to hide their true identity or motivation and covertly use a relationship to obtain information and disclose it to the local authority (an undercover officer); or

ii. A member of the public who provides a tip-off to a local authority and is asked to go back and obtain further information by establishing or continuing a relationship whilst hiding their true motivation (an informant).

There may be occasions where certain individuals are required to provide information to public authorities out of professional or statutory

duty or a member of the public volunteers a piece of information as a one off. Any such disclosures should not result in these individuals meeting the definition of a CHIS.

All applications for a CHIS must be considered and conducted in accordance with the most up to date CHIS Code of Practice.

4.3 Vulnerable individuals (a person who is in need of Regulatory care services by reason of mental or other disability, age or illness and who is or may be unable to take care or protect himself against significant harm or exploitation) may be authorised to act as a CHIS **only in the most exceptional circumstances.** Authorisation must be given by the Chief Executive or in his/her absence the Deputy Chief Executive and he or she will only do so after taking advice from the Monitoring Officer.

4.4 Authorisation will only be given for the use of a covert human intelligence source, when the activity is necessary to prevent or detect crime.

4.5 Authorisations will only be given to officers who have undergone appropriate training in human rights and the Act.

4.6 CHIS authorisations by Local Authorities are now subject to judicial approval. Local authorities need to obtain an order approving the grant of a CHIS authorisation from a Justice of the Peace.

5.0 PART 3 - COMMUNICATIONS DATA

5.1 The term ‘communications data’ embraces the ‘who’, ‘when’ ‘where’ ‘how’ and ‘with whom’ of a communication but not the content, not what was said or written. It is information about a communication - not the communication itself.

5.2 The Council will only authorise the acquisition of service use and entity information. Under no circumstances will the council obtain traffic data or intercept communications data under RIPA.

5.3 Communications data is governed by RIPA, the Investigatory Powers Act 2016 and more recently the Data Retention Acquisition Regulations 2018. These new regulations introduce a higher threshold to be able to obtain communications data. Guidance on this is set out in the Communications Data Code of Practice 2018. A request for a RIPA authorisation or notice will be scrutinised by a single point of contact (a ‘SPoC’). Local Authorities are not able to intercept communications data. Where communications data is required then responsibility for its acquisition rests with the Office for Communications Data Authorisation (OCDA). - National Anti-Fraud Network (NAFN) provide the SPoC service for Local Authorities and any application to the OCDA must be submitted through the NAFN with whom Cumberland Council has an agreement. NAFN have issued guidance which must be followed when considering any application, up to date guidance can be obtained from NAFN website.

5.4 The Council must keep records of all decisions and outcomes from the OCDA as these records are not kept centrally.

5.5 Under s.6 IPA 2016 it is against the law for a business to intercept any electronic communication on its, or anyone else's, system. There are some exceptions to this:

- Interception is authorised under a warrant (this does not apply to local authorities)
- where the interception takes place with consent
- where the interception is connected with the operation of the communications service itself
- where it is carried out by businesses for monitoring and record-keeping purposes

5.6 Interception for business related workplace monitoring may be applicable in certain circumstances by the Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000. The regulations are designed to meet the legitimate needs of businesses to manage their information systems, making use of the capabilities of modern communications technology, but in a way that is consistent with high standards of privacy.

5.7 Interception of Council telecommunications will only be made in accordance with the Regulations, and following procedures agreed by the Chief Officer. Interception may be carried out in the following circumstances:

i. To establish the existence of facts or to ascertain compliance with regulatory or self-regulatory practices (e.g. to keep records of communications where the specific facts are important, such as being able to prove that a customer has been given certain advice).

ii. To check that standards are being achieved or ought to be achieved (e.g. to check the quality of e-mail responses sent by members of staff to customer enquiries or for staff training).

iii. To prevent or detect crime (e.g. to check that employees or others are not involved in defrauding the Council).

iv. To investigate or detect unauthorised use of the telecommunications system. Note that interception that is targeted at personal communications that do not relate to the business is not allowed regardless of whether the use of the system for such communications is authorised.

v. To ensure the security of the system and its effective operation (e.g. to check for viruses or other threats to the system or to enable automated processes such as caching or load distribution).

vi. In the interests of public safety.

vii. For the purposes of preventing death or injury or any damage to a person's physical or mental health, or of mitigating any injury or damage to a persons physical or mental health;

viii. Where a person "P" has died or is unable to identify themselves because of a physical or mental condition to assist in identifying "P" or to obtain information about P's next of kin or other persons connected with P or about the reason for P's death or condition.

5.8 The Council will make all reasonable efforts to inform potential users that interceptions may be made.

6.0 Internet and Social Networking Sites and other surveillance activity that does not meet the test for RIPA authorisation.

6.1 It is recognised that the use of the internet and, in particular, social networking sites, can provide useful information for council staff carrying out investigations or gathering evidence when dealing with service users. It may in some circumstances amount to Directed Surveillance and may interfere with a person's Article 8 rights. Any officer using the internet should follow the separate guidance at Appendix 1 of this policy "Guidance on the Use of Social Networking Sites for Investigations/Evidence Gathering"

6.2 It is also recognised that council staff may be engaged in surveillance activity which does not meet the threshold for authorisation under RIPA (as set out in Part 1 – Directed Surveillance, section 3 of this policy). This may be because the offence or matter being investigated does not meet the criminal threshold of 6 months imprisonment or does not form part of the Council's core functions. An example of this would be surveillance of an employee for a disciplinary matter. Where this is the case to ensure human rights compliance, the investigator must use the same forms as if making an application under RIPA and follow the process set out in Appendix 5 of this policy.

7.0 Authorisation

7.1 At the start of an investigation, council officers will need to satisfy themselves that what they are investigating is a criminal offence. Directed surveillance is an invasive technique and at the point it is

decided whether or not to authorise its use it must be clear that the threshold is met and that it is necessary and proportionate to use it.

7.2 The council officer will complete a written RIPA authorisation or notice form setting out for consideration by the Senior Lawyer, who will act as 'gatekeeper' as defined in paragraph 8.4 below. This must provide sufficient information to enable the Senior Lawyer to consider the proposed application and discuss with the applicant whether they can obtain the information by using techniques other than covert surveillance. The decision of the Senior Lawyer should be recorded in writing on the written RIPA authorisation or notice form. If the Senior Lawyer is satisfied that the threshold is met then the council officer will submit the written RIPA authorisation or notice form to the Chief Officer.

7.3 If the council officer is authorised to proceed with their application it then must be submitted to the Chief Officer on the prescribed form which must set out why use of a particular technique is necessary and proportionate in their investigation. The Chief Officer will consider the application, recording his/her considerations and countersign the form if he/she believes the statutory tests are met.

7.4 Where the request relates to the acquisition of communications data the completed forms will be sent to the National Anti-Fraud Network (NAFN) in the role as appointed Single Point of Contact (SPoC). NAFN will review the application and if satisfied will return the application to the Chief Officer to make any necessary application to the magistrates court.

7.5 In cases where, through the use of surveillance, it is likely that knowledge of confidential information will be acquired, the use of surveillance is subject to a higher level of authorisation. The Chief Executive or in his/her absence the deputy Chief Executive will authorise surveillance activity where confidential information is likely to be acquired, he or she will do so only after taking advice from the relevant Chief Officer.

7.6 "Confidential information" is defined for the purposes of RIPA as matters subject to legal privilege, confidential personal information or confidential journalistic material. Confidential material must not be copied or retained unless for a specific purpose – e.g. use in evidence in proceedings and may only be disseminated following advice from the relevant Chief Officer.

7.7 After the form has been countersigned the local authority will seek judicial approval for their RIPA authorisation or notice. The Justice of the Peace (JP) will decide whether a local authority grant or renewal of an authorisation or notice to use RIPA should be approved and it will not come into effect unless and until it is approved by a JP.

7.8 The time limits for authorised applications are three months for directed surveillance and twelve months for a CHIS (one month if the CHIS is under 18). Authorisations and notices for communications data will be valid for a maximum of one month from the date the JP has approved the grant. This means that the conduct authorised should have been commenced or the notice served within that month.

7.9 All authorisations once granted remain the responsibility of the relevant Chief Officer. Their usage and continued applicability should be reviewed by the Chief Officer on a weekly basis and this should be recorded on the authorisations.

7.10 All authorisations should be cancelled at the end of 3 months or as soon as they have served their original purpose or once they no longer meet the criteria for continued use, whichever is the earlier. Authorisations cannot last for more than 3 months and if this is required then a new authorisation must be sought. The date of cancellation should be recorded on the authorisation.

7.11 All information and data gathered remains the responsibility of the relevant Chief Officer who must ensure that the information is kept confidentially and in accordance with the Council's records and retention policy.

7.12 The forms for completion are those available from the Home Office Website: RIPA forms - GOV.UK (www.gov.uk)

8.0 Responsibilities

8.1 **Chief Officers** to:

i. Ensure all regulatory staff are aware of and trained in the Act.

ii. Delegate the task of authorising surveillance operations where appropriate.

iii. Ensure that the forms and procedures detailed in any Investigations Manuals within their teams are kept up to date and comply with RIPA and the draft Codes of Practice.

iv. Act as the authorising officer for CHIS or DS or for communications data the designated person to consider applications, and issue, renew, cancel or refuse authorisations relating to investigations of Council employees, in accordance with the criteria set out in the Act and in Guidance from the Investigatory Powers Commissioner (IPC). Note that, when knowledge of confidential information is likely to be acquired or when a vulnerable individual or juvenile is to be used as a source, the authorisation level will be the Head of Paid Service or (in their absence) the person acting as Head of Paid Service.

v. Ensure applications are complete and are made out on the appropriate *pro forma*, except in the case of emergency applications.

vi. Maintain a record of applications and authorisations, and provide copies to the Monitoring Officer within 5 working days of the application, irrespective of whether the authorisation is granted, and copies of all cancelled authorisations within 5 working days of the cancellation.

vii. Ensure all staff involved in surveillance operations have access to the relevant Codes of Practice.

viii. Review authorisations at least weekly and record the review on the authorisation and ensure that authorisations are cancelled as soon as they have either served their original purpose or no longer meet the criteria for issue, whichever is the earlier.

8.2 **Monitoring Officer** to:

Fulfil the role of senior responsible officer for RIPA and will be responsible for:

i. The integrity of processes for the management of CHIS.

ii. Compliance with Chapter II of Part I of RIPA (Acquisition and Disclosure of Communications Data).

iii. Compliance with Part II of RIPA (Surveillance and Covert Human Intelligence Sources).

iv. Oversight of the reporting of errors to the Investigatory Powers Commissioner, identification of the cause(s) of errors and the implementation of processes to minimise repetition of errors.

v. Engagement with the Commissioners' inspectors when they conduct their inspections.

vi. Oversight of the implementation of post-inspection action plans approved by the relevant Commissioner.

vii. Maintaining a log of all RIPA applications, authorisations etc. including copies of all completed forms, and reviewing the quality of applications, authorisations etc.

viii. Ensuring that all authorising officers are of an appropriate standard in light of any recommendations made by Inspectors' reports.

ix. Ensuring that members of the Executive members and Standards and Governance Committee have sufficient understanding of human rights and RIPA to be able to discharge their responsibilities

x. Ensuring that this Policy is reviewed by Executive at least once a year and any Authorisations granted are reported to the Standards and Governance Committee annually.

xi. In the absence of the Chief Officer act as authorising officer to receive and consider applications, and issue, renew, cancel or refuse such applications relating to investigations of Council employees, in accordance with the criteria set out in the Act.

xii. Provide procedures to be adopted in the application for, granting etc. of, and recording of authorisation.

xiii. Ensure copies of the Codes of Practice for Covert Surveillance, The Use of Covert Human Intelligence Sources, and Acquisition and Disclosure of Communications Data are available for public reference at council offices or by post or e-mail on public request. https://www.gov.uk/government/organisations/home-office

xiv. Ensure that details of the complaints procedure involving the Investigatory Powers Tribunal are readily available for public reference purposes at council offices or by post or e-mail on public request.

8.4 **Senior Lawyer** to:

i. Act as a gatekeeper to ensure compliance with the relevant statutory requirements, codes of practice and this policy before any application is presented for authorisation to any Chief Officer.

8.5 **All staff involved in surveillance operations** to:

i. Be familiar with Act, the relevant Codes of Practice, and the Investigatory Powers Commissioner Guidance for Inspections.

ii. Ensure that the authorising officer is provided with all relevant information available to the investigation to enable an informed decision to be made.

iii. Advise the authorising officer as soon as practicable when an operation unexpectedly interferes with the privacy of an individual who is not the subject of the surveillance.

iv. Cease the surveillance operation immediately if no longer meets the authorisation criteria.

v. Ensure that they follow the appropriate service work instructions and guidance.

Relevant Background Papers

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

Codes of Practice made under RIPA issued by the Home Office:
https://www.gov.uk/government/collections/ripa-codes

Guidance to local authorities RIPA Codes:
https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/118173/local-authority-england-wales.pdf

Home office guidance for Magistrates Courts in England & Wales for Local Authorities
https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/118174/magistrates-courts-eng-wales.pdf

Data and Intelligence Services – General Awareness Briefing (issue 1 June 2019 as updated)
www. nafn.gov.uk

Appendix 1

GUIDANCE ON THE USE OF THE INTERNET INCLUDING SOCIAL NETWORKING SITES FOR INVESTIGATIONS/GATHERING EVIDENCE

INTRODUCTION

It is recognised that the use of the internet and, in particular, social networking sites, can provide useful information for council staff carrying out investigations or gathering evidence when dealing with service users. This guidance is aimed to support officers in their use of the internet and ensure legal compliance when doing so.

Failure to seek appropriate authorisation when necessary could result in the Council breaching an individual's right to privacy (Article 8 of the Human Rights Act) and/or amount to covert directed surveillance. It is therefore important that officers adhere to the Council's policy in respect of The Regulation of Investigatory Powers Act ('RIPA Policy') and this guidance when considering accessing internet and social networking sites as part of an investigation or to gather evidence.

It may not always be necessary to obtain RIPA authorisation, however in these cases management authorisation must be obtained by completing the form and log at appendix 2. Guidance can be found at appendix 3.

THE POLICY

The Council's RIPA Policy states:

6.1 The use of the internet and social networking sites may be required to gather information prior to and/or during an investigation, which may amount to directed surveillance, and may interfere with a person's Article 8 rights.

6.2 If an overt account on a one-off occasion is used to gather information or evidence then no authorisation is considered necessary.

6.3 If a service intends to conduct covert surveillance on an individual or site by regularly visiting and monitoring activity and it is considered that private information is likely to be obtained then a RIPA Directed Surveillance Authorisation will be required. The service would also have to consider creating a covert account to carry out this work. In addition where a service may need to communicate covertly online, for example contacting individuals, a CHIS authorisation will be required.

DEFINITION OF A SOCIAL NETWORKING SITE

It is not possible to provide a definitive list of social networking sites, so this should be taken to mean any site which involves individuals creating a profile which contains personal information and is viewable by others, whether

accepted as “friends” or otherwise. This might include sites such as ‘Facebook’ ‘Linked-In’, “Twitter” and “Instagram”.

The internet, including the use of search engines can in some circumstances result in the obtaining of private information about individuals.

The definition of ‘private information’ under the Regulation of Investigatory Powers Act (‘RIPA’) includes:

“*any information relating to a person’s private or family life and 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.”*

It is important to note that images of people are private information. Those conducting investigations should also be aware that it is possible to obtain information about other individuals, not just the specific user on the profiles which are viewed, captured, or recorded.

Sites used to advertise goods and services should be included within the definition. Although there is likely to be a reduced expectation of privacy with this type of site, there is still the possibility of obtaining private information which may be subsequently used in any proceedings.

PROCESS TO BE FOLLOWED WHEN CONSIDERING USING SOCIAL NETWORKING SITES IN INVESTIGATIONS OR TO GATHER EVIDENCE

Where an officer considers it necessary to view a social networking site or otherwise conduct research on the internet to investigate an allegation which may result in the obtaining of private information about an individual, the process to be followed is:

1 Officers must not use their own personal or private account when accessing social networking sites for investigations/intelligence gathering, only Council accounts should be used.

2 The Communications team will arrange access through a Senior Officer designated by the Chief Officer for each service area for the purposes of using social media accounts “Designated Senior Officer”. No fake profiles should be created. Use of an established, overt account of the Council on the site to look at publicly available information on the profile is appropriate as this makes the Council overt in its presence.

3 Before accessing information, the Designated Senior Officer will complete the Internet Research Form/Impact Assessment at Appendix 2 which will be submitted for approval to the Senior Lawyer.

4 Officers may access the main page of an individual’s profile or do a one off search through a search engine to take an initial view as to whether there is any substance to the allegation of the matter being investigated. The initial viewing must be reasonable, for example, where information

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

5 It would not be reasonable to spend any significant amount of time searching through various pages of an individual's profile or to print out several pages just in case they may reveal something useful. Any subsequent visit to a profile will require authorisation and the completion of the Internet Research Form at Appendix 2.

Example 1: An officer undertakes a simple internet source on a name address or telephone number to find out whether a subject of interest has an online presence. This is unlikely to need an authorisation. However, if having found an individual's social media profile or identity is decided to monitor it or extract information from it for retention in a record because it is relevant to an investigation or operation. authorisation should then be considered.
Example 2: An officer makes an initial examination of an individual's online profile to establish whether they are of relevance to an investigation. This is unlikely to need an authorisation. However, if during that initial examination it is intended to extract and record information to establish a profile including information such as identity, pattern of life, habits, intentions or associations, it may be advisable to have in place an authorisation even for that single visit. (As set out in the following paragraph, the purpose of the visit may be relevant as to whether an authorisation should be sought)
Example 3: An officer undertakes general monitoring of the internet in circumstances where it is not part of a specific, ongoing investigation or operation to identify themes, trends possible indicators or criminality or other factors that may influence operational strategies or deployments. This activity does not require RIPA authorisation, however when this activity leads to the discovery of previously unknown subjects of interest, once it is decided to monitor those individuals as part of an ongoing operation or investigation authorisation should be considered.

5. The designated Senior Officer viewing a social networking site must keep a log (Appendix 2) to record when social networking sites are viewed for investigations/evidence gathering. Each service area is responsible for regularly reviewing these logs and providing the log in a report to the Monitoring Officer for review on a quarterly basis. The Monitoring Officer will keep a central log to enable the Council to monitor the use of these sites for investigations/evidence gathering and use this information to review policies and guidance.

6. If in the course of monitoring or viewing a site, it becomes apparent that the offence being investigated falls under RIPA (see Paragraph 3.2 of the Council's RIPA policy), a formal RIPA application must be completed, authorised by one of the Council's Authorising Officers and then approved by a Magistrate.

Appendix 2

Internet Research Form/Impact assessment

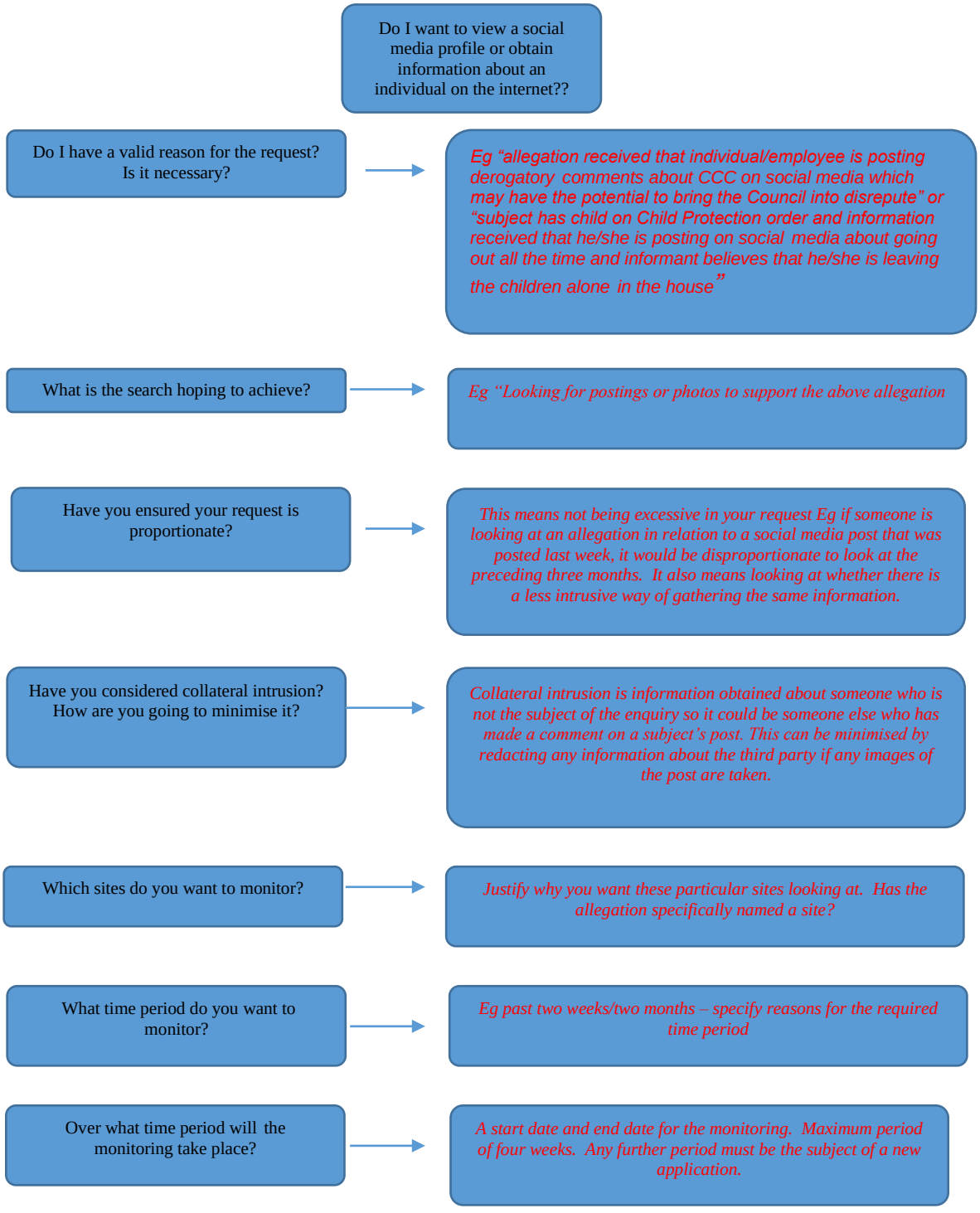
Ref no:	**Department:**	**Date:**
Subject of the research (if known) **Name** **DOB or age** **Address**		
Offence/incident or reason for the research:		
Why it is necessary to undertake the internet research and how will it benefit the enquiry?		
Is this action proportionate? **Can this information be sourced in less intrusive way?**		
Have you considered collateral intrusion? How are you going to remove or minimise it?		
Which sites do you want to monitor?		
What time period do you want to monitor?		
For how long do you want the monitoring to take place?		
Who do you need to inform about the monitoring?		
Senior Lawyer : Approved/rejected (delete as appropriate) **Any restrictions or modifications to request?**		
Signed by Designated Senior officer:		
Date:		
Signed by Senior Lawyer		
Date:		

INTERNET RESEARCH ACTIVITY LOG

This log must be used by the Designated Senior Officer to record the research undertaken. It should include all sites visited, and contain rationale for continuing the research taking into account necessity, privacy issues and proportionality. It must be submitted to the Monitoring Officer for the Central Log once completed.

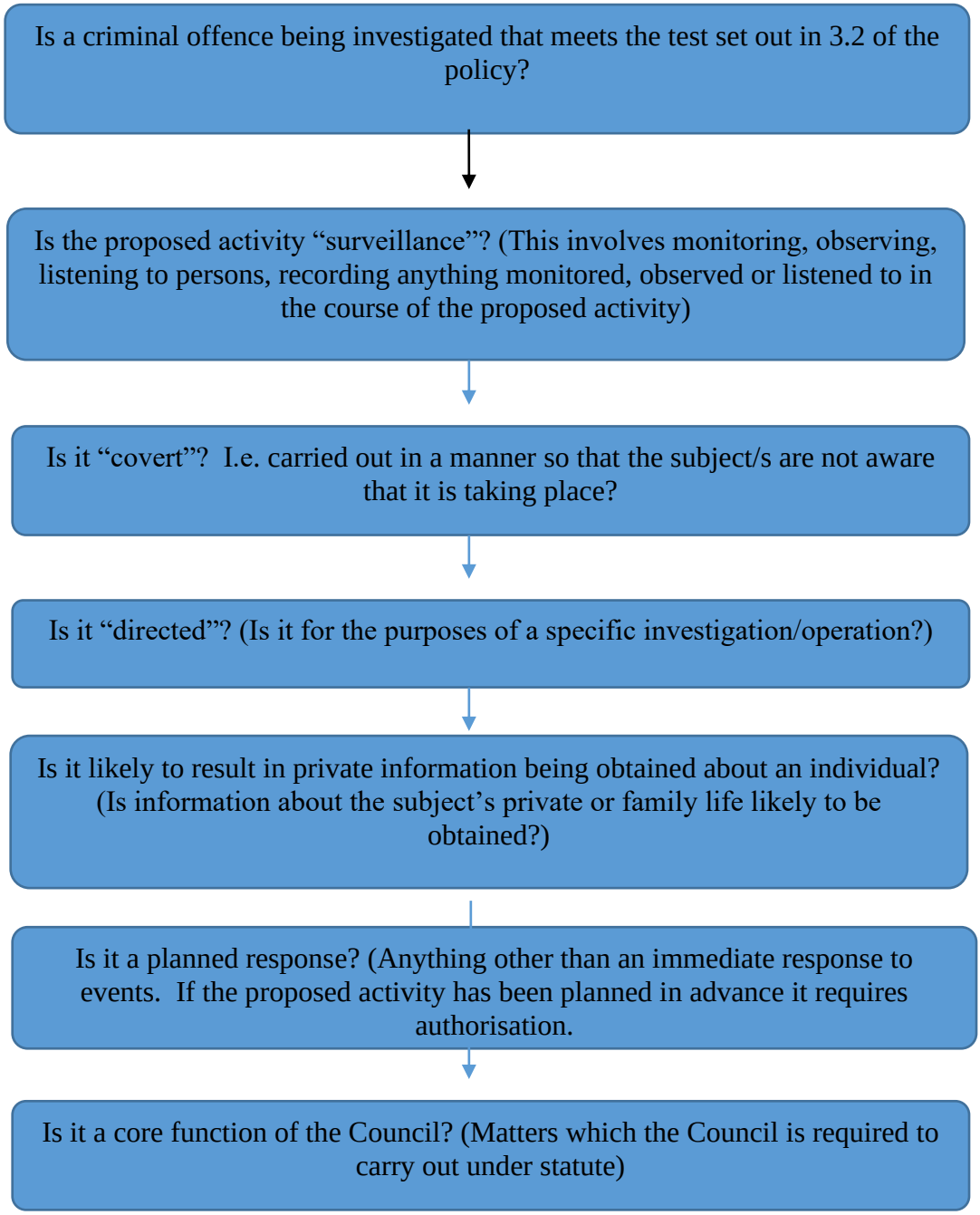
Internet Research Activity Log (to be submitted to the Monitoring Officer once completed)		
Date	Activity undertaken including sites visited	By whom

Appendix 3 SOCIAL MEDIA REQUEST FLOWCHART GUIDE – NON RIPA



IS RIPA AUTHORISATION REQUIRED?

If the answer is "no" to ANY of the questions below, the proposed activity falls outside the scope of RIPA. It may however fall within the Non-RIPA process at Appendix 5.



APPENDIX 5 – Non - RIPA Process

This process is to be used when conducting surveillance where the tests in Appendix 4 are met but it does not fall within RIPA because either :

1) it is not a criminal offence that is being investigated (as set out in 3.2 of the policy)

OR

2) it does not relate to a core function of the Council (ie: it is not a matter which the Council is required to carry out under statute)

1. The council officer will complete a written RIPA authorisation or notice form. The forms for completion are those available from the Home Office Website: RIPA forms - GOV.UK (www.gov.uk)

2. This must set out sufficient information to enable the Senior Lawyer to consider the proposed application and discuss with the applicant whether they can obtain the information by using techniques other than covert surveillance. The decision of the Senior Lawyer should be recorded in writing on the written RIPA authorisation or notice form. If the Senior Lawyer is satisfied that the threshold is met then the council officer will submit the written RIPA authorisation or notice form to the Chief Officer.

3. If the council officer is authorised to proceed with their application it then must be submitted to the Chief Officer on the prescribed form which must set out why use of a particular technique is necessary and proportionate in their investigation. The Chief Officer will consider the application, recording his/her considerations and countersign the form if he/she believes the statutory tests are met.

4. In cases where, through the use of surveillance, it is likely that knowledge of confidential information will be acquired, the use of surveillance is subject to a higher level of authorisation. The Chief Executive or in his/her absence the deputy Chief Executive will authorise surveillance activity where confidential information is likely to be acquired, he or she will do so only after taking advice from the relevant Chief Officer.

5. “Confidential information” is defined for the purposes of RIPA as matters subject to legal privilege, confidential personal information or confidential journalistic material. Confidential material must not be copied or retained unless for a specific purpose – e.g. use in evidence in proceedings and may only be disseminated following advice from the relevant Chief Officer.

6. All authorisations once granted remain the responsibility of the relevant Chief Officer. They must be sent to the Monitoring Officer for recoding on the central log. Their usage and continued applicability should be

reviewed by the Chief Officer on a weekly basis and this should be recorded on the authorisations.

7. All authorisations should be cancelled at the end of 3 months or as soon as they have served their original purpose or once they no longer meet the criteria for continued use, whichever is the earlier. Authorisations cannot last for more than 3 months and if this is required then a new authorisation must be sought. The date of cancellation should be recorded on the authorisation.

8. All information and data gathered remains the responsibility of the relevant Chief Officer who must ensure that the information is kept confidentially and in accordance with the Council's records and retention policy.