North East Derbyshire District Council

REGULATION OF INVESTIGATORY POWERS ACT 2000 (RIPA)

CORPORATE POLICY AND PROCEDURES

CONTROL SHEET FOR REGULATION OF INVESTIGATORY POWERS ACT 2000 (RIPA) – CORPORATE POLICY AND PROCEDURES

Policy Details	Comments / Confirmation (To be updated as the document progresses)
Policy title	RIPA Corporate Policy and Procedures
Current status – i.e. first draft, version 2 or final version	Draft 1 (2025 2nd Review)
Policy author	AD Governance and Monitoring Officer
Location of policy – i.e. L-drive, shared drive	S Drive
Member route for approval	Standards Committee
Cabinet Member (if applicable)	Cllr J Birkin
Equality Impact Assessment approval date	July 2025
Partnership involvement (if applicable)	N/A
Final policy approval route i.e. Executive/ Council /Planning Committee	Standards Committee
Date policy approved	July 2025
Date policy due for review (maximum three years)	May 2026
Date policy forwarded to be included on Intranet and Internet if applicable to the public	Following Standards Committee on 2nd July.

Contents

Abbreviations

AOs	Authorising Officers who are the Managing Director and Head Of Paid Service, Director of Finance and Resources and Section 151 Officer, Director of Growth and Assets.
CCTV	Closed Circuit Television
CSP	Communications service provider
Council	North East Derbyshire District Council
CHIS	Covert Human Intelligence Sources
ECHR	European Convention on Human Rights

HRA	Human Rights Act 1998
IPCO	Investigatory Powers Commissioner's Office
NAFN	The National Anti Fraud Network
OCDA	The Office for Communications Data Authorisations
PFA	Protection of Freedoms Act 2012
IPA	Investigatory Powers Act 2016
RIPA	Regulation of Investigatory Powers Act 2000
SPoCs	Single Points of Contact for Acquisition and Disclosure of Communications Data

1.1 Introduction

1.1.1 This Corporate Policy and Procedures document is based upon the requirements of the Regulation of Investigatory Powers Act 2000 and the Home Office's Codes of Practice on Covert Surveillance and Property Interference, Covert Human Intelligence Sources and Acquisition and Disclosure of Communications Data.

1.1.2 The use of covert surveillance, covert human intelligence sources and the acquisition of service use or subscriber information in relation to communications data is sometimes necessary to ensure effective investigation and enforcement of the law. However, they should be used only rarely and in exceptional circumstances. RIPA requires that public authorities follow a clear authorisation process prior to using these powers. Authorisations granted under Part II of RIPA are subject to all the existing safeguards considered necessary by Parliament to ensure that investigatory powers are exercised compatibly with the ECHR.

1.1.3 Any potential use of RIPA should be referred to the Monitoring Officer for preliminary advice at the earliest possible opportunity. In the Monitoring Officer's absence, advice should be sought from the Deputy Monitoring Officer .

Consequences of Failing to Comply with this Policy

1.1.4 Where there is interference with Article 8 of the ECHR, and where there is no other source of lawful authority for the interference, the consequences of not following the correct authorisation procedure set out under RIPA and this Policy may result in the Council's actions being deemed unlawful by the Courts under Section 6 of the HRA or by the Investigatory Powers Tribunal, opening up the Council to claims for compensation and loss of reputation. Additionally, any information obtained that could be of help in a prosecution may be inadmissible.

1.2 Background

1.2.1 On 2 October 2000 the Human Rights Act 1998 ("HRA") made it unlawful for a local authority to breach any article of the ECHR. An allegation that the Council or

someone acting on behalf of the Council has infringed the ECHR is dealt with by the domestic courts rather than the European Court of Human Rights.

1.2.2 The ECHR states:-

(a) individuals have the right to respect for their private and family life, home and correspondence (Article 8 ECHR); and

(b) there shall be no interference by a public authority with the exercise of this right unless that interference is:-

- in accordance with the law;
- necessary; and
- proportionate

1.2.3 RIPA, which came into force on 25 September 2000, provides a lawful basis for three types of covert investigatory activity to be carried out by local authorities which activities might otherwise breach the ECHR. These activities are:-

- covert directed surveillance;
- covert human intelligence sources ("CHIS"); and
- acquisition and disclosure of communications data

1.2.4 RIPA sets out procedures that must be followed to ensure the investigatory activity is lawful. Where properly authorised under RIPA the activity will be a justifiable interference with an individual's rights under the ECHR. If the interference is not properly authorised an action for breach of the HRA could be taken against the Council, a complaint of maladministration made to the Local Government Ombudsman or a complaint made to the Investigatory Powers Tribunal. In addition, if the procedures are not followed any evidence collected may be disallowed by the courts. RIPA seeks to balance the rights of individuals against the public interest in the Council being able to carry out its statutory duties.

1.2.5 A flow chart attached at Appendix A to this policy sets out the process for covert directed surveillance and covert human intelligence sources (CHIS).

What RIPA Does and Does Not Do

1.2.6 RIPA does:-

- require prior authorisation of covert directed surveillance;
- prohibit the Council from carrying out intrusive surveillance;
- compel disclosure of communications data from telecom and postal service providers;
- permit the Council to obtain communications records from communications

service providers;

- require authorisation of the conduct and use of CHIS;
- require safeguards for the conduct of the use of a CHIS.

1.2.7 RIPA does not:-

- make conduct unlawful which is otherwise lawful;
- prejudice any existing power to obtain information by any means not involving conduct that may be authorised under RIPA. For example, it does not affect the Council's current powers to obtain information via the DVLA or to obtain information from the Land Registry as to the owner of a property;
- apply to activities outside the scope of Part II of RIPA. A public authority will only engage RIPA when in performance of its "core functions" – i.e. the functions specific to that authority as distinct from all public authorities.
- cover overt surveillance activity.

1.2.8 RIPA only applies to the Council's core functions – i.e. its statutory duties, and not staffing issues or contractual disputes.

1.2.9 Under no circumstances can local authorities be authorised to obtain communications traffic data under RIPA. Local authorities are not permitted to intercept the content of any person's communications and it is an offence to do so without lawful authority.

1.3 Policy Statement

1.3.1 The Council is determined to act responsibly and in accordance with the law. To ensure that the Council's RIPA activity is carried out lawfully and subject to the appropriate safeguards against abuse, a Corporate Policy and Procedures document has been drafted as detailed below.

1.3.2 All staff who are considering undertaking RIPA activity should be aware that where that activity may involve handling confidential information or the use of vulnerable or juvenile persons as sources of information, a higher level of authorisation is required. Please see paragraphs 2.7 (in respect of handling confidential information) and 2.9 (in respect of using information sources who are vulnerable or juvenile persons) below.

1.3.3 The following information and documents are available-

- Home Office Statutory Codes of Practice on the Gov.uk website.
- Links to RIPA forms online for covert surveillance; CHIS and acquisition and disclosure of communications data;
- Corporate RIPA Training.

1.3.4 The Monitoring Officer is the Council's Senior Responsible Officer (SRO) and is responsible for the following roles:-

- Appointing Authorising Officers (see 2.11);
- Appointing Designated Persons (see 3.4);
- Maintaining a central record for all RIPA authorisations;
- Arranging training to individuals appointed as Authorising Officers and Designated Persons, and
- Carrying out an overall monitoring function as the SRO for the Council's use of RIPA powers.

1.3.5 Any officers who are unsure about any RIPA activity should contact the Monitoring Officer for advice and assistance.

1.3.6 Where surveillance activity is carried out in relation to crimes that do not meet the RIPA Thresholds as detailed within this policy, these must be logged within individual Council departments and submitted to the Monitoring Officer on a quarterly basis. Non-RIPA Authorisations will be considered by Members as part of their Annual Report.

1.4 Social Media

1.4.1 The use of the internet may be required to gather information prior to and/or during an operation, which may amount to directed surveillance. Although information that individuals make publicly available on the internet would not normally be classed as 'private information', the Office of the Surveillance Commissioners' Annual Report 2016 states that repeated visits to individual sites may develop into surveillance activity which would require authorisation. By virtue of conducting research online, rather than using other more 'overt' methods, there may be a perception that the investigation is intended to be covert. Whenever a public authority intends to use the internet as part of an investigation, they must first consider whether the proposed activity is likely to interfere with a person's Article 8 rights. Particular consideration should be paid to the likelihood of collateral intrusion through obtaining private information about others who have not given their consent. Advice should be sought as early as possible.

1.4.2 Any activity likely to interfere with an individual's Article 8 rights should only be used when necessary and be proportionate to meet the objectives of a specific case. Where it is considered that private information is likely to be obtained, an authorisation (combined or separate) must be sought as set out elsewhere in this code. Where an investigator may need to communicate covertly online, for example, contacting individuals using social media websites, a CHIS authorisation should be considered.

1.4.3 The Council maintains detailed and specific guidance for its officers' use of social media in investigations. This forms an annex to this policy and should be referred to in all circumstances where:

- open source research is gathered;

- open source information is publicly available; and
- Information is stored for an investigation.

1.4.4 The Social Media guidance includes details as to how access to social media should be monitored to ensure compliance.

1.4.5 The Council does not ordinarily permit the use of false personas to obtain information. Any such need to do so requires the authorisations detailed in Section 2.

1.5 Training & Advice and Departmental Policies, Procedures and Codes of Conduct

1.5.1 The Monitoring Officer will arrange regular training on RIPA. All Authorising Officers, designated persons and investigating officers should attend at least one session every two years and further sessions as and when required.

1.5.2 Training can be arranged on request and requests should be made to the Monitoring Officer. In particular training should be requested for new starters within the Council who may be involved in relevant activities.

1.5.3 If officers have any concerns, they should seek advice about RIPA from the Monitoring Officer.

1.5.4 Where in practice, departments have any policy, procedures or codes of practice in relation to RIPA that are different from or in addition to this Code, they must immediately seek advice from the Monitoring Officer.

1.6 Complaints

1.6.1 Any person who believes they have been adversely affected by surveillance activity or other investigatory activity covered by RIPA by or on behalf of the Council may complain to the authority by contacting the Monitoring Officer.

1.6.2 They may also complain to the Investigatory Powers Tribunal at:-

Investigatory Powers Tribunal
PO Box 33220
London
SW1H 9ZQ

1.7 Monitoring of Authorisations

1.7.1 The Monitoring Officer is the senior responsible officer in relation to RIPA and is responsible for:-

- The integrity of the process in place to authorise directed surveillance, the use of CHIS and the acquisition and disclosure of communications data;
- Compliance with Part II of RIPA and this Policy;
- Engagement with the Investigatory Powers Act Commissioner's Office when they conduct inspections; and
- Where necessary, overseeing the implementation of any post-inspection plans recommended or approved by a Commissioner.

1.7.2 The Monitoring Officer is also required by law to ensure that the Council does not act unlawfully and will undertake audits of files to ensure that RIPA is being complied with and will provide feedback to the Authorising Officer/designated person where deficiencies in the RIPA process are noted.

1.7.3 The Monitoring Officer will invite the Standards Committee to review the Council's RIPA Policy on an annual basis and to recommend any changes to the Council's Policy or Procedures and will also provide members with an annual update on use.

1.8 Error Reporting

1.8.1 The Council is required to report 'relevant errors' to the Investigatory Powers Commissioner, which includes circumstances where the requirements of the RIPA legislation or guidance have not been met. Examples include:

- Surveillance activity has taken place without lawful authorisation
- There has been a failure to adhere to the safeguards applicable to the use of a CHIS.

1.8.2 When any officer identifies that activity that should have been authorised under RIPA may have taken place, they must notify the Monitoring Officer immediately. The officer(s) involved in the investigation will be required to provide a report on all relevant circumstances including:

- Information on the cause of the potential error
- The amount of surveillance or property interference conducted
- Nature and amount of any material obtained or disclosed
- Details of any collateral intrusion (i.e. any third party information collected in addition to that of the subject of the investigation.)
- Whether any material has been retained or destroyed

1.8.3 The Monitoring Officer will determine whether a 'relevant error' has occurred. If required, the Monitoring Officer will also give advice on steps to be taken to avoid the error recurring.

1.8.4 If the Monitoring Officer establishes that a 'relevant error' has occurred, this must be reported to the Investigatory Powers Commissioner as soon as reasonably practicable and no later than 10 days after the error has been established. If additional

time is required to ascertain the full facts of the error, an initial notification must be submitted with an estimated timetable of when the full report can be supplied.

1.8.5 The report to the Investigatory Powers Commissioner must contain the details set out at 1.8.2 as well as details of any steps taken to prevent recurrence of the error.

1.8.6 If an authorisation has been obtained on the basis of information provided by a third party that later turns out to be incorrect, but was relied upon in good faith, this error should also be notified to the Investigatory Powers Commissioner (although it does not constitute a 'relevant error' under the legislation).

1.8.7 The Home Office Guidance sets out what action the Investigatory Powers Commissioner will take following notification of relevant errors, including determining whether it is a serious error and whether the person concerned should be notified.

1.8.8 The Council has a responsibility to report to the Inspector at the commencement of an inspection all activity which should have been authorised but was not. This is to confirm that any direction provided by the Commissioner has been followed.

RIPA PART 2

COVERT SURVEILLANCE AND THE USE OF COVERT HUMAN INTELLIGENCE SOURCES

2.1 Types of Surveillance

2.1.1 Surveillance can be overt or covert and includes:-

- 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; and
- Surveillance by or with the assistance of a device.*

*More detailed guidance on the use of surveillance devices, such as cameras, microphones, vehicle tracking and drones can be found in the relevant Home Office Code of Practice.

2.1.2 Indicators of whether investigatory activity will amount to surveillance include the formality and duration of the activity and the nature of what is being observed.

2.2 Overt Surveillance

2.2.1 The majority of the Council's surveillance activity will be overt surveillance, i.e. will be carried out openly. For example (i) where the Council performs regulatory checks on licensees to ensure they are complying with the terms of any licence granted; and (ii) where the Council advises a tenant that their activities will be monitored as a result of neighbour nuisance allegations. This type of overt surveillance is normal Council business and is not regulated by RIPA.

2.3 Covert Surveillance

2.3.1 This is where surveillance is carried out in a manner calculated to ensure that the person subject to the surveillance is unaware it is taking place. Covert surveillance can be intrusive or directed. **The Council is not permitted to carry out covert intrusive surveillance.** Para 2.4 below explains when covert surveillance is intrusive and therefore not permitted. The Council is permitted to carry out covert directed surveillance subject to strict compliance with RIPA. Paragraph 2.5 below explains when covert surveillance is directed.

2.4 Covert Intrusive Surveillance

2.4.1 Covert intrusive surveillance takes place when covert surveillance is carried out in relation to anything taking place on residential premises or in a private

vehicle and which involves the presence of an individual or surveillance device on the premises or in the vehicle, or which uses a device placed outside the premises or vehicle which consistently provides information of the same quality and detail as expected of a device placed inside. Additionally, the Regulation of Investigatory Powers (Extension of Authorisations Provisions: Legal Consultations) Order 2010 states that covert surveillance carried out in relation to anything taking place in certain specified premises is intrusive when they are being used for legal consultation.

2.5 Covert Directed Surveillance

2.5.1 This is surveillance that is:-

- Covert;
- Not intrusive;
- For the purposes of a specific investigation or operation;
- Likely to obtain private information* about a person (whether or not that person was the target of the investigation or operation); and
- Not carried out as an immediate response to events or circumstances which could not have been foreseen prior to the surveillance taking place.

* Private information includes any information relating to a person's private and family life including professional and business relationships, home and correspondence (whether at home, in a public place or in the work place). Further information and examples of what is considered private information is contained at section 3 of the Home Office Code of Practice on Covert Surveillance and Property Interference.

2.6 Directed Surveillance Crime Threshold

2.6.1 Following the changes to RIPA introduced by the Protection of Freedoms Act 2012, a crime threshold applies to the authorisation of covert directed surveillance by local authorities. *(Article 7A of Regulation of Investigatory Powers (Directed Surveillance and Covert Human Intelligence Sources) Order 2010)*

2.6.2 Local Authority Authorising Officers may not authorise covert directed surveillance unless it is for the purpose of preventing or detecting a criminal offence **and** meets the following test:-

- The criminal offence is punishable by a maximum term **of at least six months imprisonment**, or

- It would constitute an offence under Sections 146, 147A of the Licensing Act 2003 or Section 7 of the Children and Young Persons Act 1993

(offences involving sale of tobacco and alcohol to underage children) regardless of length of prison term.

2.6.3 Whether or not the crime threshold is met should be kept under review during the course of the investigation. If the relevant criminal offence is downgraded and the threshold is no longer met, the authorisation for surveillance should be cancelled.

2.6.4 The crime threshold **only** applies to covert directed surveillance, not to CHIS or Communications Data.

2.6.5 The Home Office Statutory Covert Surveillance and Property Interference Code of Practice can be found on the Home Office website.

2.7 Confidential Information

2.7.1 A higher level or authorisation to apply to the Magistrates Court is required in relation to RIPA activity when the subject of the investigation might reasonably expect a high degree of privacy, or where "confidential information" might be obtained. For the purpose of RIPA this includes:-

- Communications subject to legal privilege (see below);
- Communications between a member of parliament and another person on constituency matters;
- Confidential personal information (see below); and
- Confidential journalistic material (see below).

2.7.2 The Authorising Officer and the person carrying out the surveillance must understand that such information is confidential and is subject to a stringent authorisation procedure. **Authorisation can only be granted by the Head of Paid Service**.

2.7.3 **Legal privilege** is defined in Section 98 of the Police Act 1997 as:-

- communications between a professional legal adviser and his client, or any person representing his client which are made in connection with the giving of legal advice to the client.

- communications between a professional legal adviser and his client or any person representing his client, or between a professional legal adviser or his client or any such representative and any other person which are made in connection with or in contemplation of legal proceedings and for the purposes of such proceedings.

- items enclosed with or referred to in communications of the kind mentioned above and made in connection with the giving of legal advice, or in

connection with or in contemplation of legal proceedings and for the purposes of such proceedings.

2.7.4 Communications and items are not matters subject to legal privilege when they are in the possession of a person who is not entitled to possession of them, and communications and items held, or oral communications made, with the intention of furthering a criminal purpose are not matters subject to legal privilege.

2.7.5 If advice is required on this point, officers should contact the Monitoring Officer.

2.7.6 **Confidential personal information** is described at paragraph 9.29 of the Home Office Covert Surveillance and Property Interference Code of Practice.

2.7.7 **Confidential journalistic material** is described at paragraph 9.38 of the Home Office Covert Surveillance and Property Interference Code of Practice.

2.7.8 **Any officer contemplating RIPA activity where the above circumstances may apply must seek advice from the Monitoring Officer prior to making any application.**

2.8 Covert Human Intelligence Sources ("CHIS")

2.8.1 The Council is permitted to use CHIS subject to strict compliance with RIPA.

Under the 2000 Act, a CHIS is a person who establishes or maintains a personal or other relationship with a person for the covert purposes of facilitating:-

(a) covertly using the relationship to obtain information or provide access to information to another person, or

(b) covertly disclosing information obtained by the use of the relationship or as a consequence of the existence of such a relationship.

and if the relationship is conducted in a manner that is calculated to ensure that one of the parties to the relationship is unaware of the purpose. Guidance can be obtained from the Home Office "Guidance Covert Human Intelligence revised code of practice".

2.8.2 A RIPA authorisation and order from a magistrate is required for the above activity and should be obtained whether the CHIS is a Council officer or another person who is asked to be a CHIS on the Council's behalf. Authorisation for CHIS can only be granted if it is for the purposes of "preventing or detecting crime or of preventing disorder".

2.8.3 Members of the public who volunteer information to the Council and those engaged by the Council to carry out test purchases in the ordinary course of business (i.e. they do not develop a relationship with the shop attendant and do not use covert recording devices) are not CHIS and do not require RIPA authorisation.

2.8.4 However, by virtue of Section 26(8) of RIPA, there may be instances where an individual, covertly discloses information obtained by the use of such a relationship, or as a consequence of the existence of such a relationship. In such circumstances where a member of the public, though not asked to do so, gives information (or repeated information) about a suspect, then serious consideration should be given to designating the individual as a CHIS, particularly if the Council intends to act upon the information received. It is recommended that legal advice is sought in any such circumstances.

2.9 Safety and Welfare of CHIS

2.9.1 The safety and welfare of the CHIS is paramount. Risk assessments should be carried out to determine the risk of tasking a CHIS and the activities being undertaken by the particular person appointed. The risk assessments should be regularly reviewed during the course of the investigation.

2.9.2 A single point of contact should be appointed for the CHIS to communicate with, who will be responsible for carrying out the risk assessments and taking all possible steps to ensure their safety and welfare. A senior officer should also have oversight of the arrangements and be regularly updated by officer acting as the single point of contact. Regular face-to-face meetings should occur with the CHIS rather than solely remote contact, such as telephone or email, although remote contact may be appropriate in addition.

2.10 Vulnerable Individuals/Juvenile CHIS

2.10.1 A vulnerable individual is a person who by reason of mental disorder or vulnerability, other disability, age or illness, is or may be unable to take care of themselves or protect themselves against significant harm or exploitation.

2.10.2 Additional requirements apply to the use of a vulnerable adult or a person under the age of 18 as a CHIS. In both cases **authorisation for an application to the Magistrates Court can only be granted by the Head of Paid Service. Any officer contemplating the use of a juvenile or a vulnerable person as a CHIS must seek advice from the Monitoring Officer prior to making the application.**

2.10.3 The use or conduct of a CHIS under 16 years of age **must not** be authorised to give information against their parents or any person who has parental responsibility for them. In other cases authorisations should not be granted unless the special provisions contained in The Regulation of Investigatory

Powers (Juveniles) Order 2000 are satisfied. This sets out rules about parental consent, meetings, risk assessments and the duration of the authorisation.

2.11 CCTV

2.11.1 The installation and use of unconcealed CCTV cameras for the purpose of generally observing activity in a particular area is not surveillance requiring RIPA authorisation. There are specific provisions relating to the use of CCTV cameras in public places and buildings. However, if CCTV cameras are being used in such a way that the definition of covert directed surveillance is satisfied, RIPA authorisation should be obtained.

2.11.2 For instance the use of town centre CCTV systems to identify those responsible for a criminal act immediately after it happens will not require RIPA authorisation. However, the use of the same CCTV system to conduct planned surveillance of an individual and record their movements is likely to require authorisation.

2.11.3 Protocols should be agreed with any external agencies requesting the use of the Council's CCTV system. The protocols should ensure that the Council is satisfied that authorisations have been validly granted prior to agreeing that the CCTV system may be used for directed surveillance.

2.11.4 CCTV systems cannot be used without prior production of an authorisation and such authorisations must be retained. For more details please refer to the Council's "Use of Overt Surveillance Systems Policy".

2.12 Authorisation Procedures

Authorisations given by Authorising Officers are subject to approval by the Magistrates Court (See para 2.15 below)

2.12.1 Authorising Officers are responsible for assessing and authorising covert directed surveillance and the use of a CHIS.

2.12.2 It is the responsibility of Authorising Officers to ensure that when applying for authorisation the principles of necessity and proportionality (see 2.13 below) are adequately considered and evidenced; and that reviews and cancellations of authorisations are carried out as required under this Policy (2.20 – 2.22 below).

2.12.3 Lists of Authorising Officers are set out below. Any requests for amendments to the lists must be sent to the Monitoring Officer.

2.12.4 The authorising officers for North East Derbyshire District Council are as follows:

Managing Director & Head of Paid Service – Lee Hickin (01246 217218)

Director of Finance and Resources – Jayne Dethick (01246 2417078)

Director of Growth and Assets – Matthew Broughton (01246 242210)

2.12.5 Schedule 1 of statutory instrument No 521 (2010) prescribes the rank or position of authorising officers for the purposes of Section 30(1) of RIPA (covert surveillance and CHIS). For Local Authorities they prescribe a "Director, Head of Service, Service Manager or equivalent".

2.12.6 The Monitoring Officer designates which officers can be Authorising Officers. Only these officers can authorise directed surveillance and the use of CHIS. **All authorisations must follow the procedures set out in the Policy**. Authorising officers are responsible for ensuring that they have received RIPA training prior to authorising RIPA activity. When applying for or authorising RIPA activity under the Policy, officers must also take into account the corporate training and any other guidance issued from time to time by the Monitoring Officer.

2.13 Authorisation Of Covert Directed Surveillance and use of A CHIS

2.13.1 RIPA applies to all covert directed surveillance and the use of CHIS whether by Council employees or external agencies engaged by the Council. Council officers wishing to undertake covert directed surveillance or use of a CHIS must complete the relevant application form and forward it to the relevant (para 2.12.4) Authorising Officer.

2.13.2 Any potential use of RIPA should be referred to the Monitoring Officer for preliminary advice.

2.14 Criteria for The Authorisation of the Use of RIPA Powers

2.14.1 Covert directed surveillance and/or the use of a CHIS can only be authorised if the Authorising Officer is satisfied that the activity is:-

(a) **in accordance with the law** i.e. it must be in relation to matters that are statutory functions of the Council. As such the Council is unable to access communications data for disciplinary matters.

(b) **necessary** for the purpose of preventing or detecting crime or preventing disorder. This is the only ground available to the Council for authorising RIPA activity and for directed surveillance only, there is a crime threshold as described in paragraph 2.6 above;

(c) **proportionate** to what it seeks to achieve. This involves balancing the seriousness of the intrusion into the privacy of the subject of the operation (or any other person as may be affected) against the need for the activity in investigative operational terms. Any conduct that is excessive as to the interference and the aim of the conduct, or is in any way arbitrary will not be proportionate. Serious consideration must be given to identifying the least intrusive method of obtaining the information required.

2.14.2 Applicants should ask the following types of questions to help determine whether the use of RIPA is necessary and proportionate:-

- why it is believed the proposed conduct and use is necessary for the prevention of crime or the prevention of disorder (as appropriate);
- how the activity to be authorised is expected to bring a benefit to the investigation;
- how and why the proposed conduct and use is proportionate to the intelligence dividend it hopes to achieve, having regard to the gravity and extent of the activity under investigation;
- how and why the methods to be adopted will cause the least possible intrusion to the subject/s i.e. interfere with their rights under the ECHR;
- what other reasonable methods of obtaining information have been considered and why they have been discounted.

2.14.4 When completing an application, officers must present the case in a fair and balanced way. In particular all reasonable efforts should be made to take account of information which supports or weakens the case for the authorisation.

2.14.4 Authorising Officers should not be responsible for authorising their own activities, i.e. those operations/investigations in which they are directly involved. However, it is recognised that in exceptional circumstances this may sometimes be unavoidable. The Monitoring Officer should be informed in such cases.

2.14.5 Particular consideration should be given to **collateral intrusion on or interference with the privacy of persons who are not the subject(s) of the investigation.** Collateral intrusion occurs when an officer undertaking covert surveillance on a
subject observes or gains information relating to a person who is not the subject of the investigation. An application for an authorisation must include an assessment of the risk of any collateral intrusion or interference and measures must be taken to avoid or minimise it. This must be taken into account by the Authorising Officer, particularly when considering the proportionality of the surveillance.

2.14.6 Particular care must be taken in cases where **confidential information** is involved

e.g. matters subject to legal privilege, confidential personal information, confidential journalistic material, confidential medical information, and matters relating to religious leaders and their followers. In cases where it is likely that confidential information will be acquired, officers must specifically refer this to the Monitoring Officer for advice.

2.15 Processing the authorisation

2.15.1 At the time of authorisation the Authorising Officer must set a date for review of the authorisation and review it on that date (see 2.19), prior to the authorisation lapsing as it must not be allowed to lapse.

2.15.2 The original completed application and authorisation form must be forwarded to the Monitoring Officer as soon as possible. The Monitoring Officer will maintain a central register of the Council's RIPA activity and a unique reference number will be allocated to each application. This will be kept in Legal Services.

2.16 Approval by Magistrates Court

2.16.1 Under the Protection of Freedoms Act 2012, there is an additional stage in the process for investigatory activities (covert directed surveillance and CHIS). After the authorisation form has been countersigned by the Authorising Officer, the Council is required to obtain judicial approval for either the authorisation or a renewal of an authorisation.

2.16.2 For arrangements for submitting applications to the Magistrates, please contact Legal Services.

2.16.3 The magistrate will have to decide whether the Council's application to grant or renew an authorisation to use RIPA should be approved and it will not come into effect unless and until it is approved by the Magistrates Court.

2.16.4 A separate application should be completed when the Council is requesting judicial approval for the use of more than one of the surveillance techniques (i.e. Directed Surveillance, CHIS and Communications Data) at the same time.

2.16.5 It should be noted that only the initial application and any renewal of the application require magistrates' approval.

2.16.6 There is no requirement for officers presenting authorisations to the Magistrates Court to be legally qualified but they do need to be authorised by the Council to represent it in court. **Generally the applicant should be accompanied to Court by the Authorising Officer and a member of the Legal Team.**

2.17 The Role of the Magistrates Court

2.17.1 The role of the Magistrates Court is set out in Section 32A RIPA (for directed surveillance and CHIS).

2.17.2 This section provide that the authorisation shall not take effect until the Magistrates Court has made an order approving such authorisation. The matters on which the Magistrates Court needs to be satisfied before giving judicial approval are that:-

- There were reasonable grounds for the local authority to believe that the authorisation or notice was necessary and proportionate;

- In the case of a CHIS authorisation, that there were reasonable grounds for the local authority to believe that:

    - arrangements exist for the safety and welfare of the source that satisfy Section 29(5) RIPA;
    - the requirements imposed by Regulation of Investigatory Powers (Juveniles) Order 2000 were satisfied;

- The local authority application has been authorised by an Authorising Officer;

- The grant of the authorisation was not in breach of any restriction imposed by virtue of an order made under the following sections of RIPA:

- o 29(7)(a) (for CHIS),

- o 30(3) (for directed surveillance and CHIS).

Summary of procedure for applying for covert directed surveillance or use of a CHIS is:

- Applicant obtains preliminary legal advice from Monitoring Officer;
- Applicant completes an application;
- Monitoring Officer quality checks the completed application before approving it to go to the Authorising Officer;
- Approval is sought from the Authorising Officer;
- Authorising Officer completes authorisation form in long-hand;
- Monitoring Officer organises paperwork for court and the applicant, the Authorising Officer proceeds to court, accompanied by a member of the legal team wherever possible;

- If approval given, applicant organises the covert directed surveillance or use of a CHIS to take place;
- Original copy of application lodged with Legal Team.

Additional Requirements for Authorisation of a CHIS

A CHIS must only be authorised if the following arrangements are in place:-

- There is a Council officer with day-to-day responsibility for dealing with the CHIS and a senior Council officer with oversight of the use made of the CHIS;
- A risk assessment has been undertaken to take account of the CHIS security and welfare;
- A Council officer is responsible for maintaining a record of the use made of the CHIS;
- Any adverse impact on community confidence or safety regarding the use of a CHIS has been considered, taking account of any particular sensitivities in the local community where the CHIS is operating; and
- Records containing the identity of the CHIS will be maintained in such a way as to preserve the confidentiality or prevent disclosure of the identity of the CHIS.

2.18 Urgent Authorisations

2.18.1 By virtue of the fact that an authorisation under RIPA is not approved until signed off by a Magistrates Court, urgent oral authorisations are not available.

2.19 Application Forms

2.19.1 Only the RIPA Forms listed below can be used by officers applying for RIPA authorisation.

(a) Directed Surveillance

- Application for Authority for Directed Surveillance
- Review of Directed Surveillance Authority
- Cancellation of Directed Surveillance
- Renewal of Directed Surveillance Authority

(b) CHIS

- Application for Authority for Conduct and Use of a CHIS

- Review of Conduct and Use of a CHIS
- Cancellation of Conduct and Use of a CHIS
- Renewal of Conduct and Use of a CHS

2.20 Duration of the Authorisation

2.20.1 Authorisation/notice durations are:-

- for covert directed surveillance the authorisation remains valid for three months after the date of authorisation;
- for a CHIS the authorisation remains valid for 12 months after the date of authorisation (or after four months if a juvenile CHIS is issued);

2.20.2 Authorisations should not be permitted to expire, they must be either renewed or cancelled when the activity authorised has been completed or is no longer necessary or proportionate in achieving the aim for which it was originally authorised. This is a statutory requirement which means that all authorisations must be reviewed to decide whether to cancel or renew them.

2.21 Review of Authorisations

2.21.1 As referred to at 2.15.1 Authorising Officers must make arrangements to periodically review any authorised RIPA activity. Officers carrying out RIPA activity, or external agencies engaged by the Council to carry out RIPA activity, must periodically review it and report back to the Authorising Officer if there is any doubt as to whether it should continue. Reviews should be recorded on the appropriate Home Office Form (see 2.18).

2.21.2 A copy of the Council's notice of review of an authorisation must be sent to the Monitoring Officer as soon as possible to enable the central record on RIPA to be authorised.

2.22 Renewal of Authorisations

2.22.1 If the Authorising Officer considers it necessary for an authorisation to continue they may renew it for a further period, beginning with the day when the authorisation would have expired but for the renewal. They must consider the matter again taking into account the content and value of the investigation and the information so far obtained, considering the same criteria as for new applications (see 2.13 above). Renewed authorisations will normally be for a period of up to three months for covert directed surveillance or 12 months in the case of CHIS, one month in the case of juvenile CHIS. Authorisations may be renewed more than once, provided they are considered again and continue to meet the criteria for authorisation. Applications for the renewal of an authorisation for covert directed surveillance or CHIS authorisation must be made on the appropriate form (see 2.18).

2.22.2 All renewals will require an order of the Magistrates Court in accordance with the requirements in para 2.17 above.

2.22.3 A copy of the Council's notice of renewal of an authorisation must be considered by the Monitoring Officer before it is made and all original copies lodged with the Legal Team together with a copy of the Magistrates Court order renewing the authorisation to enable the central record on RIPA to be updated.

2.23 Cancellation of Authorisations

2.23.1 The person who granted or last renewed the authorisation must cancel it when they are satisfied that the covert directed surveillance or CHIS no longer meets the criteria for authorisation. Cancellations must be made on the appropriate Home Office Form (see 2.18).

2.23.2 A copy of the Council's notice of cancellation of an authorisation must be sent to the Monitoring Officer within one week of the cancellation to enable the central record on RIPA to be updated.

2.24 What happens if the surveillance has unexpected results?

2.24.1 Those carrying out the covert surveillance should inform the Authorising Officer if the investigation unexpectedly interferes with the privacy of individuals who are not the original subjects of the investigation or covered by the authorisation. In some cases the original authorisation may not be sufficient to cover the activity required or information likely to be gathered and in such cases, consideration should be given as to whether a separate authorisation is required.

2.25 Records and Documentation

Departmental Records

2.25.1 Applications, renewals, cancellations, reviews and copies of notices must be retained by the Council in written or electronic form, and physically attached or cross-referenced where they are associated with each other. These records will be confidential and should be retained for a period of at least five years from the ending of the authorisation. Where it is believed that the records could be relevant to pending or future court proceedings, they should be retained and then destroyed five years after last use.

Central Record of Authorisations, Renewals, Reviews and Cancellations

2.25.2 A joint central record of directed surveillance and CHIS is maintained by the Monitoring Officer at the District Council Offices, Mill Lane, Wingerworth.

2.25.3 The central record is maintained in accordance with the requirements set out in the Home Office Codes of Practice. In order to keep the central record up-to-date Authorising Officers must, in addition to sending through the Home Office application, authorisation form and Magistrates Court order as soon as possible following the authorisation being approved by the Magistrates Court (see 2.15) send notification of every renewal, cancellation and review on the Council's notification forms (see 2.19 – 2.22).

2.25.4 Using the information on the central record the Monitoring Officer will:-

- remind Authorising Officers in advance of the expiry of authorisations;
- remind Authorising Officers of the need to ensure surveillance does not continue beyond the authorised period;
- remind Authorising Officers to regularly review current authorisations;
- on the anniversary of each authorisation, remind Authorising Officers/delegated persons to consider the destruction of the results of surveillance operations.

2.26 Surveillance products

2.26.1 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 for a suitable further period, commensurate to any subsequent review.

2.26.2 Particular attention is drawn to the requirements of the Codes of Practice issued under the Criminal Procedure and Investigations Act 1996 by the Home Office and on the Home Office website. These require that material which is obtained in the course of a criminal investigation and which may be relevant to the investigation must be recorded and retained.

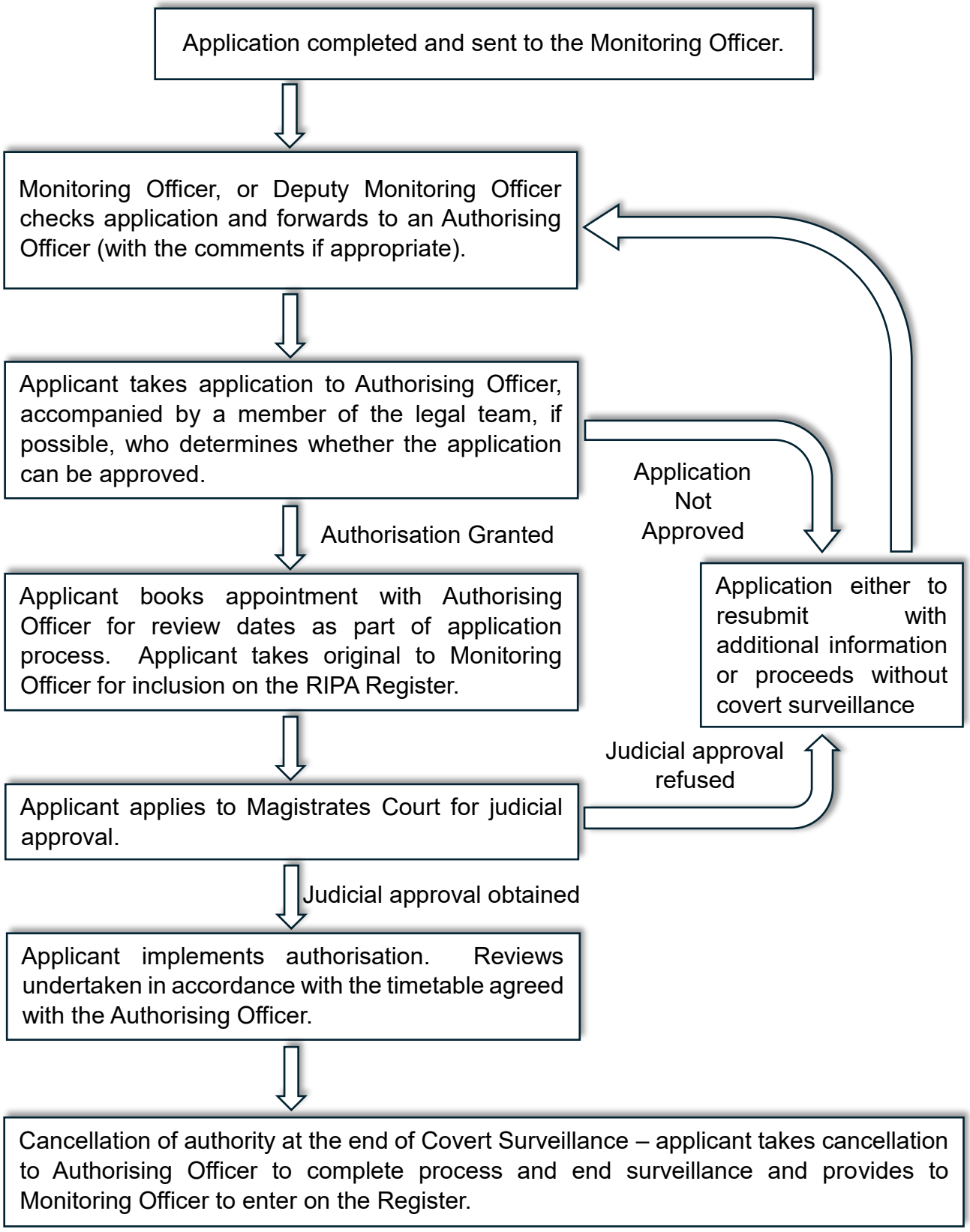
2.26.3 There is nothing in RIPA which prevents material obtained from properly authorised surveillance from being used in other investigations. The Council will ensure that adequate arrangements are in place for the handling and storage of material obtained through the use of covert surveillance to facilitate its use in other investigations.

2.26.4 Material obtained through the use of directed surveillance or CHIS containing personal information will be protected by the Data Protection Act 2018 (DPA) and in addition to the considerations above must be used, stored and destroyed in compliance with the appropriate requirements of the DPA and the Council's Data Protection, Information Security and Records Management Policies.

2.26.5 Dissemination, copying and retention of material must be limited to the minimum necessary for authorised purposes. See section 9 of the Home

Office Code of Practice for more detail of the safeguards that must be in place. Particular protection must be given to confidential or privileged information.

APPENDIX A - RIPA PROCESS FLOWCHART



RIPA PART 1 – CHAPTER 2
ACQUISITION AND DISCLOSURE OF COMMUNICATIONS DATA

3.1 Permitted Purposes for Acquisition and Disclosure of Communications Data

3.1.1 Local authorities are only permitted to acquire communications data for the purposes of preventing or detecting serious crime. Other purposes are permitted for other public bodies. Currently this Authority has not used these powers.

3.1.2 A 'serious crime' is an offence that is punishable by a maximum term of imprisonment of 12 months or more.

3.2 Communication Service Providers ("CSPs")

3.2.1 CSPs are organisations that are involved in the provision, delivery and maintenance of communications such as postal, telecommunication and internet service providers but also, for example, hotel or library staff involved in providing and maintaining email access to customers. The Council must obtain communications data from CSPs in strict compliance with RIPA.

3.3 Types of Communications Data

3.3.1 Communications data is the "who", "where", "when" and "how" of a communication such as a letter, phone call or email but not the content, not what was said or written. The Council is not able to use RIPA to authorise the interception or acquisition of the content of communications. There are three types of communication data:-

Service Use Information

3.3.2 This is data relating to the use made by any person of a postal or telecommunications, internet service, or any part of it. For example itemised telephone call records, itemised records of connection to internet services, itemised timing and duration of calls, connection/disconnection/reconnection data, use of forwarding or re-direction services, additional telecom services and records of postal items.

Subscriber information

3.3.3 This is information held or obtained by the CSP about persons to whom the CSP provides or has provided a communications service. For instance, subscribers of email and telephone accounts, account information including payment details, address for installing and billing, abstract personal records and sign up data.

Traffic Information

3.3.4 This is data that is comprised in or attached to a communication for the purpose of transmitting it and which identifies a person or location to or from which it is transmitted. **The Council is not permitted to access traffic data.**

3.4 Use of Communications Data

3.4.1 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 as they are not empowered to do so.

3.4.2 Communications data is governed by the Regulation of Investigatory Powers 2000, (RIPA) the Investigatory Powers Act 2016 (IPA) and the Data Retention Acquisition Regulations 2018. These regulations introduced a higher threshold to be able to obtain communications data. Guidance on this is set out in the Home Office Communications Data Code of Practice 2025. 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 this Council has an agreement. When consideration is given to obtaining communications data, the guidance from NAFN should be obtained from the Section 151 Officer of the Deputy Section 151 Officer and used in connection with the application.

3.4.3 NAFN have issued guidance which must be followed when considering any application. This guidance can be obtained from the NAFN website. Where consideration is being given to obtaining communications data, in addition to contacting the Monitoring Officer, the guidance from the NAFN should be obtained from the Section 151 Officer or the Deputy Section 151 Officer and used in connection with the application.

3.4.3 The Council must keep records of all decisions and outcomes from the OCDA as these records are not kept centrally. These will be kept on the RIPA Register by the Monitoring Officer.

3.5 Authorisation of Acquisition and Disclosure of Communications Data

3.5.1 Any potential use of RIPA should be referred to the Monitoring Officer for preliminary advice.

3.6 Urgent Authorisations

3.6.1 By virtue of the fact that an authorisation under RIPA is not approved until signed off by a Magistrates Court, urgent oral authorisations are not available.

3.7 Central Record of Authorisations, Renewals, Reviews and Cancellations

3.7.1 A joint central record of access to communications data authorisations is maintained by the Monitoring Officer at the District Council Offices, Mill Lane, Wingerworth.

3.7.2 See paragraph 2.24 for more information on the central records, which also apply in relation to covert surveillance and CHIS.

3.7.3 Material obtained through acquisition of communications data containing personal information will be protected by GDPR and the Data Protection Act (DPA) and in addition to the considerations above must be used, stored and destroyed in compliance with the appropriate requirements of the GDPR/DPA and the Council's Data Protection, Information Security and Records Management Policies.

North East Derbyshire District Council

Guidance on the Use of Social Media in Investigations

Background

The Council has an approved Corporate Policy and Procedures Document on the Regulation of Investigatory Powers Act 2000 (RIPA). For all relevant bodies, RIPA arrangements and their use fall under the oversight of the Investigatory Powers Commissioner's Office (IPCO), which assumed responsibility from the former Office of Surveillance Commissioners (OSC) in September 2017 and the Council may be subject to a periodic inspection to ensure that it complies with legislation and guidance.

In the reports for the Councils, (these were joint inspections with Bolsover District Council) both 2013-14 and 2014-15, comment was raised on the use of social networks in investigations as follows:

2013-14 report

"This is now a deeply embedded means of communication between people and one that public authorities can exploit for investigative purposes."

"Although there remains a significant debate as to how anything made publicly available in this medium can be considered private, my Commissioners remain of the view that the repeat viewing of individual 'open source' sites for the purpose of intelligence gathering and data collation should be considered within the context of the protection that RIPA affords to such activity."

"I strongly advise all public authorities empowered to use RIPA to have in place a corporate policy on the use of social media in investigations."

2014-15 report

"Public authorities now make use of the wide availability of details about individuals, groups or locations that are provided on social networking sites and a myriad of other means of open communication between people using the Internet and their mobile communication devices."

"I repeat my view that just because this material is out in the open, does not render it fair game. The Surveillance Commissioners have provided guidance that certain activities will require authorisation under RIPA and this includes repetitive viewing of what are deemed to be 'open source' sites for the purpose of intelligence gathering and data collation."

"My inspections have continued to find instances where social networking sites have been accessed, albeit with the right intentions for an investigative approach, without any corporate direction, oversight or regulation."

In August 2018, the Home Office issued its Revised Code of Practice covering Covert Surveillance and Property Interference and this now includes a section on 'online covert activity'. This guidance has been reviewed in 2024 and the guidance can be viewed at paragraph 3.10 onwards.

A copy of the full guidance can be found at: Covert surveillance and property interference code of practice (accessible) - GOV.UK

This corporate guidance document has been developed to assist officers in ensuring their investigations are carried out lawfully.

General RIPA Information

The guidance states that:-

> *"The Internet is a surveillance device as defined by RIPA section 48(1). Surveillance is covert 'if, and only if' it is conducted in a manner that is calculated to ensure that persons who are subject to the surveillance are unaware that it is, or may be, taking place.' Knowing that something is happening is not the same as an awareness that it is or may be taking place."*

While activity involving the use of social networks in an investigation may be deemed to be surveillance, within the meaning of RIPA (S.48(2)), not all will require a RIPA authorisation (or qualify for the protection offered through RIPA compliance – i.e. it may not reach the crime threshold).

Most cases which officers investigate will not meet the crime threshold for a RIPA authorisation. RIPA use now not only requires the internal approval of an Authorising Officer but also that of a magistrate.

This test is set out within the Council's RIPA policy.

Where a proposed investigation does not relate to an activity that meets the crime threshold, the Council expects officers to follow a similar procedure for assessment, evidencing necessity / proportionality and internal Authorising Officer review in order to provide a documented trail as a defence in the event of subsequent litigation.

Although failure to obtain appropriate authorisation or undertake a proper assessment does not render surveillance automatically unlawful, it could lead to any evidence obtained being deemed inadmissible and/or civil action taken against the Council /

Officers for breach of the subject's right to privacy under Article 8 of the European Convention on Human Rights.

The Convention qualifies this right so that in certain circumstances the Council may interfere in that person's right if that interference is:- • in accordance with the law;

- necessary; **and**
- proportionate.

Depending upon the circumstances, the IPCO and the Home Office have advised that accessing or use of information found on social media, could be classed as Covert Directed Surveillance or the use of a Confidential Human Intelligence Source (CHIS) on a case by case basis:-

- Covert Directed Surveillance means surveillance which is carried out in such a way that the person(s) subject to it is unaware that it is or may be taking place.
- As a result of the Protection of Freedoms Act, from 1 November 2012 Directed Surveillance authorisations will have a crime threshold applied whereby local authorities can only authorise use of directed surveillance under RIPA to prevent or detect criminal offences that are either punishable, whether on summary conviction or indictment, by a maximum term of at least 6 months' imprisonment or are related to the underage sale of alcohol and tobacco.
- A person is a Covert Human Intelligence Source (CHIS) if they establish or maintain a relationship with another person in order to:-
  - covertly obtain information;
  - provide access to information to a third party; or
  - covertly disclose information obtained by the use of such a relationship and the other person is unaware that the purpose of the relationship is one of the above.

Information on the Internet

Online communication via the internet has, in recent years, become the preferred method of communication with other individuals, within social groups or with anyone in the world with internet access. Such communication may involve web sites, social networks (e.g. Facebook), chat rooms, information networks (e.g. Twitter) and/or web based electronic mail.

Just because other people may also be able to see it or access the information, does not necessarily mean that a person has no expectation of privacy in relation to that information.

Observing, monitoring and obtaining private information can amount to covert surveillance and therefore an interference with a person's right to respect for their private and family life.

Many officers and staff will have considerable experience of using the internet for their own personal online research. However managers should ensure that staff members carrying out online research and investigation for the Local Authority are both competent and appropriately trained. Any online research and investigation leaves a trace or 'footprint' and therefore safeguards need to be put in place to protect staff but also adequate procedures need to be in place to ensure such interrogation is undertaken lawfully.

Council Guidance

Open Source Research is the collection, evaluation and analysis of materials from sources available to the public, whether on payment or otherwise, to use as intelligence or evidence within investigations.

Open Source Information is publicly available information (i.e. any member of the public could lawfully obtain the information by request or observation). It includes books, journals, TV and radio broadcasts, newswires, internet WWW and newsgroups, mapping, imagery, photographs, commercial subscription databases and grey literature (conference proceedings and institute reports).

The Council's corporate approach is that it is acceptable for officers to undertake open source research and access open source information for the purposes of investigations / research in respect of individuals or businesses if undertaken properly, in accordance with council policy and in accordance with the law.

Investigations

If an officer during an investigation, deems it necessary and proportionate to use Open Source Research or collate Open Source Information (and such investigation does not meet the crime threshold for authorisation via RIPA), such use must be subject to adequate consideration and authorisation(s) which will depend upon the activity being undertaken.

Recording, storing and using restricted access information, in order to build up a profile of a person or a group of people must be both necessary and proportionate, and it must

be retained and processed in accordance with the principles of the GDPR and DPA legislation.

Appendix 3 provides a general guide for officers.

Privacy Controls

The initial interaction involved in the act of bypassing privacy controls (the sending and acceptance of a friend's request) may not by itself, meet the RIPA definition of a "relationship" and will not require authorisation as a Covert Human Intelligence Source (CHIS), but such practise is discouraged. Officers are encouraged to use other means of investigating.

The creation of a false persona involving other "friends", which are also false, in order to effect the deception and secure the information effectively amounts to "legend building" in support of the CHIS and would require proper authorisations. Again this is discouraged.

Under no circumstances should an investigating officer encourage inappropriate, fraudulent or criminal behaviour in order to provoke a response as part of the use of social networking facilities in ANY of the circumstances described above.

Officers must not set up bogus accounts/identities without further discussion with the RIPA Authorising Officer and/or Legal Services and such activity will be discouraged.

Prior Notification

Unless you seek the proper authority from the Magistrates Court for permission to use covert surveillance techniques, prior notification of the use of social media in investigations should be given. Suitable wording can be provided by Legal Services

Access to Social Media Accounts

Officers should not use personal or private accounts to access social media for the purposes of investigations.

One specified Corporate Social Media Account will be used for the purposes discussed above. Such account will not use a false identity.

The communications team will monitor the sites although there will be a clear post on the site advising individuals that the site is not monitored and will redirect them to use the customer services email/telephone number.

Such site will only be used to carry out searches and not to comment, friend or "like" certain pages. Officers can screen shot information relevant to their investigation, in accordance with the table set out above and recorded in the table as set out in appendix 2.

When is Authorisation for Social Media Use Required

Research activity does not need to be authorised or recorded **except** where it relates to an investigation by any Service Area. For example, the communications team would not normally need to record their social media usage unless they are requested to access social media on behalf of another service as part of an investigation.

No social media investigations should be carried out without prior knowledge of the relevant Service Manager (where relevant) and authorisation of someone more senior than the investigating officer.

Single visit or casual research on social media does not need to be recorded, however, where there are repeated visits to a premises or visits to a specific web page or facebook page a log should be retained and initialled by the Service Manager to confirm their authorisation for the activity.

The following should be recorded on a log with the following information:

- Officer carrying out the research
- Target of the investigation
- Date/time of viewing
- Information obtained from social platform
- Why it was considered that the viewing was necessary
- Pages saved and where saved to
- Authorisation from the Service Manager (or substitute)

The template log attached to this policy at appendix 2 should be used unless the information identified above can be recorded on a team's own "working" system (for example ECINS) so long as the information can be effectively extracted for the purposes of reporting to the IPCO or Members.

Logs will be reviewed quarterly by the Governance Manager on behalf of the Monitoring Officer and anonymised statistics will be reported to Members annually as part of the RIPA report.

Advice to Officers

As noted elsewhere in this guidance document, there are some grey areas over the legitimate use of social networking in investigations and the IPCO themselves have recognised that "there is a fine line between general observation, systematic observation and research."

If an Officer is considering the use of social networking for such activity, or is uncertain as to how to proceed, then further advice on the guidance and the potential RIPA requirements may be obtained from:-

- RIPA Authorising Officers
- Monitoring Officer
- Governance Manager

- Legal Services Manager

Associated Documents

This guidance is linked to a number of other Council documents which are available to staff via the Extranet:-

- RIPA Policy and Procedures Document
- Social Media Management Guidance – from Communications
- Policy on Social Networking – from Human Resources
- Links to Home Office Statutory Codes of Practice online
- Links to Office of the Surveillance Commissioners' Guidance Procedures online
- Links to RIPA forms online for covert surveillance; CHIS and acquisition and disclosure of communications data; Corporate RIPA Training.
- Further information on the ICO Employment Practices Code may be obtained from the Information Commissioner's Office website:- https://ico.org.uk/media/fororganisations/documents/1064/the_employment_practices_code.pdf

Appendix 1

Extract from Home Office Code of Practice - Covert Surveillance and Property Interference
February 2024

Online covert activity

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

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

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

3.13 As set out in paragraph 3.14 below, depending on the nature of the online platform, there may be a reduced expectation of privacy where information

relating to a person or group of people is made openly available within the public domain, however in some circumstances privacy implications still apply. This is because the intention when making such information available was not for it to be used for a covert purpose such as investigative activity. This is regardless of whether a user of a website or social media platform has sought to protect such information by restricting its access by activating privacy settings.

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

3.15 Whether a public authority interferes with a person's private life includes a consideration of the nature of the public authority's activity in relation to that information. Simple reconnaissance of such sites (i.e. preliminary examination with a view to establishing whether the site or its contents are of interest) is unlikely to interfere with a person's reasonably held expectation of privacy and therefore is not likely to require a directed surveillance authorisation. But where a public authority is systematically collecting and recording information about a particular person or group, a directed surveillance authorisation should be considered. These considerations apply regardless of when the information was shared online. See also paragraph 3.6.

***Example** 1: A police officer undertakes a simple internet search 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, it 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: A customs 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 visit 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: A public authority undertakes general monitoring of the internet in circumstances where it is not part of a specific, ongoing investigation or 20 operation to identify themes, trends, possible indicators of 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.

3.16 In order to determine whether a directed surveillance authorisation should be sought for accessing information on a website as part of a covert investigation or operation, it is necessary to look at the intended purpose and scope of the online activity it is proposed to undertake.

Factors that should be considered in establishing whether a directed surveillance authorisation is required include:

- Whether the investigation or research is directed towards an individual or organisation;
- Whether it is likely to result in obtaining private information about a person or group of people (taking account of the guidance at paragraph 3.6 above);
- Whether it is likely to involve visiting internet sites to build up an intelligence picture or profile;
- Whether the information obtained will be recorded and retained;
- Whether the information is likely to provide an observer with a pattern of lifestyle;
- Whether the information is being combined with other sources of information or intelligence, which amounts to information relating to a person's private life;
- Whether the investigation or research is part of an ongoing piece of work involving repeated viewing of the subject(s);
- Whether it is likely to involve identifying and recording information about third parties, such as friends and family members of the subject of interest, or information posted by third parties, that may include private information and therefore constitute collateral intrusion into the privacy of these third parties.

3.17 Internet searches carried out by a third party on behalf of a public authority, or with the use of a search tool, may still require a directed surveillance authorisation (see paragraph 4.32).

***Example**: Researchers within a public authority using automated monitoring tools to search for common terminology used online for illegal purposes will not normally require a directed surveillance authorisation. Similarly, general analysis of data by public authorities either directly or through a third party for predictive purposes (e.g. identifying crime hotspots or analysing trends) is not usually directed surveillance. In such cases, the focus on individuals or groups is likely to be sufficiently cursory that it would not meet the definition of surveillance. But officers should be aware of the possibility that the broad thematic research may evolve, and that authorisation may be appropriate at the point where it begins to focus on specific individuals or*

groups. If specific names or other identifiers of an individual or group are applied to the search or analysis, an authorisation should be considered.

Extract from Home Office Code of Practice - Covert Human Intelligence Sources
December 2022

Online Covert Activity

4.29 Any member of a public authority, or person acting on their behalf, who conducts activity on the internet in such a way that they may interact with others in circumstances where the other parties could not reasonably be expected to know their true identity, should consider whether the activity requires a CHIS authorisation. This applies whether the interaction involves publicly open websites such as an online news and social networking service, or more private exchanges such as messaging sites. Where the activity is likely to result in obtaining private information but does not amount to establishing or maintaining a CHIS relationship, consideration should be given to the need for a directed surveillance authorisation.

4.30 Where someone, such as an employee or member of the public, is tasked by a public authority to use an internet profile to establish or maintain a relationship with a subject of interest for a covert purpose, or otherwise undertakes such activity on behalf of the public authority, in order to obtain or provide access to information, a CHIS authorisation is likely to be required. For example:

- an investigator using the internet to engage with a subject of interest at the start of an operation, in order to ascertain information or facilitate a meeting in person;
- directing a member of the public to use their own or another internet profile to establish or maintain a relationship with a subject of interest for a covert purpose;
- joining chat rooms with a view to interacting with a criminal group in order to obtain information about their criminal activities.

4.31 A CHIS authorisation will not always be appropriate or necessary for online investigation or research. Some websites require a user to register providing personal identifiers (such as name and phone number) before access to the site will be permitted. Where a member of a public authority sets up a false identity for this purpose, this does not in itself amount to establishing a relationship, and a CHIS authorisation would not immediately be required. However, consideration should be given to the need for a directed surveillance authorisation if the conduct is likely to result in the acquisition of private information, and the other relevant criteria are met.

Example 1: An HMRC officer intends to make a one-off online test purchase of an item on an auction site, to investigate intelligence that the true value of the goods is not being declared for tax purposes. The officer concludes the purchase and does not correspond privately with the seller or leave feedback on the site. No covert relationship is formed, and a CHIS authorisation need not be sought.

Example 2: HMRC task a member of the public to purchase goods from a number of websites to obtain information about the identity of the seller, country of origin of the goods and banking arrangements. The individual is required to engage with the seller as

necessary to complete the purchases. The deployment should be covered by a CHIS authorisation because of the intention to establish a relationship for covert purposes.

4.32 Where a website or social media account requires a minimal level of interaction, such as sending or receiving a friend request before access is permitted, this may not in itself amount to establishing a relationship. Equally, the use of electronic gestures such as “like” or “follow” to react to information posted by others online would not in itself constitute forming a relationship. However, it should be borne in mind that entering a website or responding on these terms may lead to further interaction with other users and a CHIS authorisation should be obtained if there is an intention to engage in such interaction to obtain, provide access to or disclose information.

Example 1: An officer maintains a false persona, unconnected to law enforcement, on social media sites in order to facilitate future operational research or investigation. As part of the legend building activity he “follows” a variety of people and entities and “likes” occasional posts without engaging further. No relationship is formed, and no CHIS authorisation is needed.

Example 2: An officer who has maintained a false persona uses that persona to send a request to join a closed group known to be administered by a subject of interest, connected to a specific investigation. A directed surveillance authorisation would be likely to be appropriate in respect of the proposed covert monitoring of the site if the activity is likely to result in obtaining private information. Once accepted into the group it becomes apparent that further interaction is necessary: this should be authorised by means of a CHIS authorisation.

4.33 When engaging in conduct as a CHIS, a member of a public authority should not adopt the identity of a person known, or likely to be known, to the subject of interest or users of the site without considering the need for a CHIS authorisation. Full consideration should be given to the potential risks posed by that activity.

4.34 Where use of the internet is part of the tasking of a CHIS, the risk assessment carried out in accordance with paragraphs 7.15 to 7.21 of this Code should include consideration of the risks arising from that online activity including factors such as the length of time spent online and the material to which the CHIS may be exposed. This should also take account of any disparity between the technical skills of the CHIS and those of the handler or Authorising Officer, and the extent to which this may impact on the effectiveness of oversight.

4.35 Where it is intended that more than one person will share the same online persona, each individual should be clearly identifiable within the overarching authorisation for that operation. The authorisation should provide clear information about the conduct required of – and the risk assessments in relation to – each individual involved. (See also paragraphs 3.32 to 3.36).

Appendix 2

LOG – Accessing Social Media

Officer and designation accesing social media	Date/time	Social media type	Reason/purpose/ why is it necessary?	Means of notification of access to infromation	Information retained / used	Action taken e.g. CPW, prosecution, injunction	Senior officer signature

Appendix 3

Notes (if in doubt seek advice) -

Nature of Activity	**Assessment Required**	**Log/Records Required**	**Possible RIPA Authorisation**
Communications Research – browsing (monitoring) 3rd party posts on social networking sites / feeds (e.g. Facebook, X/Twitter, Instagram etc.) solely for the purposes of identifying comments (positive or negative) about the Council and its activities (as is also undertaken for newspapers) is a research activity for sharing information with our residents and businesses from partner organisations such as Derbyshire Police, traffic/weather updates, community events etc.	No	No	No
Casual (one-off) examination of public posts on social networks as part of investigations undertaken	No	Yes Simple form listing sites/targets	No
Repetitive examination/monitoring of public posts as part of an investigation	Yes Authorisation from officer more senior than the investigating officer	Yes	May be classed as Directed Surveillance. Seek advice if unsure.
Examination / use of any ostensible 'private' mechanisms on social networks (e.g. as a	Yes Authorisation from Service Manager	Yes	Yes Directed Surveillance or the use of CHIS

Nature of Activity	Assessment Required	Log/Records Required	Possible RIPA Authorisation
'friend' on Facebook, use of 'private' messaging on X (Twitter), etc.):- • within an existing relationship where the parties are known to each other, but information is freely obtained is used or passed on to an appropriate area for use in an investigation • through a new relationship set up in an open manner (i.e. in the name of the Council)			
Any Covert activity such as the following circumstances: • where a relationship is set up in a 'covert' manner specifically to obtain information • a person know to the subject becomes a 'friend', etc. specifically fo the purposes of investigation • a person becomes a 'friend', etc. in a false of misleading name • where a dialogue is entered into in order to elicit information for the investigation with the subject remaining unaware (as this may be classed as entrapment).	Yes Must inform RIPA authorising officer/Monitoring Officer	Yes	Yes Directed Surveillance and/or the use of a CHIS