Appendix

North Lincolnshire Council

Policy and Procedures Document

on

The Regulation of Investigatory Powers Act 2000

(RIPA)

January 2023

Contents Page

NORTH LINCOLNSHIRE COUNCIL RIPA POLICY

1. Introduction

The Regulation of Investigatory Powers Act 2000 (RIPA) came into force on 25 September 2000. The Act introduced a system of authorisation which will serve to secure the lawfulness of surveillance activities and ensure they are consistent with the Council's obligations under the Human Rights Act 1998.

As well as the Act itself, several sets of Regulations have been produced along with two Home Office Codes of Practice.

1.1 Human Rights Act 1998

Section 6 of the Human Rights Act makes it unlawful for the Council to act in any way that is incompatible with the European Convention for the Protection of Human Rights (ECHR).

Article 8 of the ECHR provides:

1. Everyone has the right to respect for his private and family life, his home and his correspondence.
2. There shall be no interference by a public authority with the exercise of this right except such as is:
   - i) in accordance with the law; and
   - ii) is necessary in a democratic society in the interests of public safety, prevention of disorder or crime, protection of health or morals and protection of the rights and freedoms of others.

Therefore, surveillance will breach a person's human rights unless it is authorised under RIPA. RIPA provides the legal framework for lawful interference.

1.2 Ensuring compliance with RIPA

The rights of its citizens are paramount to North Lincolnshire Council. In order to protect these rights whilst exercising its powers under RIPA, the Council has recognised that it is vital for effective procedures to be put in place and for them to be continuously monitored and reviewed. These procedures will ensure good practice is used throughout the Council and that a balance is struck between the administration of justice and the rights of the public.

The Council has prioritised the following objectives in its aim to carry out full implementation of its statutory duties:

- To ensure an awareness of RIPA amongst Council staff
- To ensure Council staff appreciate how RIPA may affect their work practices
- To establish a forum for the dissemination of information to employees and the public using the Council's website
- To ensure that appropriate training is received by its employees in order that staff are fully able to comply with the law.

1.3 The scope of this policy document

This document explains:

- The Council's statutory responsibility to comply with RIPA when undertaking covert surveillance, using a covert human intelligence source (a CHIS) and accessing communications data.
- What "covert surveillance" and "covert human intelligence source" mean.
- What is meant by communications data and how it can be accessed
- Issues which Council employees must consider under RIPA
- The procedure Council employees need to follow when applying for RIPA authorisations.

1.4 North Lincolnshire Council's statutory responsibility

The Council has a statutory responsibility to comply with the Human Rights Act 1998 and the ECHR as discussed above.

Any monitoring, observing, or listening to individuals or accessing their communications data will infringe their rights. Officers of North Lincolnshire Council can only interfere if such interference is in accordance with the law, is necessary and is proportionate. Obtaining a RIPA authorisation ensures that an officer has properly considered the private information that may be obtained, the necessity and proportionality of the surveillance, and whether it complies with the subject's human rights. A RIPA authorisation can only be granted for the purpose of preventing and/or detecting crime or disorder. There are no other grounds under which a council may grant a RIPA authorisation.

Officers should note that RIPA authorisations are only required in respect of covert surveillance. Overt surveillance falls outside the RIPA regime. Overt surveillance is that which is open and not secret or concealed. If the required result can be achieved by overt surveillance, this option should be considered.

2. Covert Surveillance

Surveillance is monitoring, observing, or listening to persons, their movements, conversations or other activities or communications, or recording any of the above activities. If you are conducting surveillance in a way calculated to ensure that the person is unaware of your actions, this is covert surveillance (as opposed to overt surveillance to which RIPA doesn't apply).

There are two types of surveillance:

- **Directed Surveillance** – This is surveillance undertaken for the purpose of a specific operation and in a manner which is likely to result in the obtaining of private information about a person (whether or not

that person is the target of the investigation or operation); and is carried out in a planned manner and not by way of an immediate response.

- **Intrusive Surveillance** – This is surveillance that takes place on residential premises or any private vehicle and involves the presence of an individual on the premises or in the car, or by the use of a surveillance device that although not in the car/premises, provides data as though it was.

In no circumstances does RIPA authorise the carrying out of any form of intrusive surveillance by local authorities.

Examples:

- An observation post using binoculars outside premises which provides a limited view and no sound of what is happening inside the premises would not be intrusive surveillance, but would be directed surveillance and require a RIPA authorisation because the surveillance would be targeted at an individual.
- You think a milkman is employing a 12yr old delivery boy in the early morning and want to follow the milk van to establish this. This would be directed surveillance and you will need a RIPA authorisation to do this.
- You have reason to believe a single person who is claiming housing and Council tax benefit is living with an undeclared partner. You need to watch the house to see if the partner is residing there, this will be directed surveillance and will require a RIPA authorisation.

Reference should be made to the Home Office Code of Practice when considering Directed Surveillance (Appendix A)

2.1 Applying for a Directed Surveillance RIPA authorisation

If you believe that your intended actions fall under the definition of directed covert surveillance, you will need to apply for a RIPA authorisation. You will need to make an application on the relevant form which should be downloaded from the Home Office website, **www.homeoffice.gov.uk/counter-terrorism/regulation-investigatory-powers**

Application forms for directed surveillance will need to contain the following information:

- The action that needs to be authorised
- An explanation of why the surveillance is necessary, *which includes reference to the criminal offences which are being investigated and whether these offences carry a sentence of 6 months imprisonment or more*
- If known, the identities of the people who are going to be the subject of the directed surveillance
- An account of the investigation
- An explanation of the techniques that you intend to use
- Confirmation that the action proposed is intended to prevent crime or detect crime and/or disorder
- An explanation of why the directed surveillance is considered to be proportionate to the outcome it seeks to achieve
- An explanation of the information which is hoped to be obtained
- An assessment of the potential for collateral intrusion (i.e, what interference will there be with the privacy of persons other than the subjects of the surveillance
- Whether any confidential information will be acquired

Note: Standard wording should not be used when completing authorisations. The explanation and information provided on the authorisation should relate to the individual facts of the case and state clearly the objectives of the surveillance.

The 3 key elements of any RIPA authorisation are **necessity, proportionality** and whether there is any risk of **collateral intrusion.** Before the Authorising Officer authorises the RIPA application, he will need to be sure that the authorisation is necessary for the purpose of preventing or detecting crime or preventing disorder, that the surveillance is proportionate to the outcome sought, and that any risk of collateral intrusion has been identified and minimised. *The necessity element of the application should embrace a consideration of why the use of the covert surveillance is actually necessary to the investigation.*

The surveillance activity will not be proportionate if it is excessive in the circumstances of the case or if the information could be reasonably obtained by other less intrusive means. In the "Proportionality" section of the application, the officer should include a consideration of the following three elements, a) that the proposed covert surveillance is proportionate to the mischief under investigation; b) that it is proportionate to the degree of anticipated intrusion on the target and others; and c) it is the only option, other overt means having been tried or considered and discounted. The Officer submitting the application will need to detail the problem that the surveillance is seeking to solve and the extent of any intrusion that may occur.

As stated above, officers will need to state on the application form the nature of the activities to be undertaken. **If during the course of the operation those activities change, a new authorisation will need to be applied for.** A flowchart detailing the Council's internal procedure can be found at **Appendix B**.

3. Covert Human Intelligence Source (CHIS)

A CHIS is another way of obtaining information and requires a RIPA authorisation.

A CHIS is any person who establishes or maintains a personal or other

relationship with a person for the covert purpose of using such a relationship either to obtain information or provide access to information about another person.

A relationship is covert if it is conducted in a manner to ensure that one party is unaware of its purpose.
A typical test purchase exercise, which does not go beyond what would be considered to be a normal transaction, would not need to be authorised as a CHIS activity.

A CHIS situation would arise where a person makes a number of contacts with the target of the investigation in order to build up a relationship of trust or familiarity before making a purchase or asking for an action to be done. A CHIS authorisation would also be required if the activity suggested was beyond the usual activity that would be carried out by any normal consumer in a shop, such as asking non routine questions to the target in an attempt to find out more information about them or the alleged crime.

There is no use of a CHIS merely because a person offers information to the local authority that may be material to the investigation of an offence.

3.1 Applying for a CHIS authorisation under RIPA

Applications for authorisations to use a CHIS must be made on the relevant Home Office form found at **www.homeoffice.gov.uk/counter-terrorism/regulation-investigatory-powers** and include the following:

- Details about the purpose for which the CHIS will be used
- The identity, where known, to be used by the CHIS
- Details of what the CHIS will be asked to do
- Details of the investigation
- Why the use of a CHIS is considered to be proportionate
- Explanation of the information it is hoped will be obtained

- The potential for collateral intrusion (i.e, interference with the privacy of people who aren't subjects in the investigation.

- Likelihood of acquiring any confidential information

Officers making a CHIS application and Authorising Officers should be aware of and have regard to the relevant Home Office Code of Practice. (Appendix C)

Note: As with directed surveillance application forms, standard wording should not be used when completing authorisations.
Before granting an authorisation, the Authorising Officer must be satisfied that the authorisation is necessary for the purpose of preventing and detecting crime, or preventing disorder, and also that it is necessary to use a CHIS in this investigation. The Officer must also believe that using a CHIS is proportionate to the outcome sought and that there are adequate procedures in place for maintaining records of the operation. Collateral Intrusion will also need to be considered.

When using a CHIS, the Authorising Officer and the officer who made the application must have regard to section 29(5) of RIPA and also to The Regulation of Investigatory Powers (Source Records) Regulations 2000.
These provisions provide (amongst other things) the following:

- There will at all times be an officer within the Council who will have day to day responsibility for the CHIS
- There will be another officer within the Council who is responsible for record keeping regarding the CHIS
- There will be another officer within the Council who will have general oversight over the use made of the CHIS
- That records will document significant information connected with the security and welfare of the CHIS
- That the tasks given to the CHIS and the uses made of the CHIS are recorded.

- The identity of the CHIS and the identity that is used by the CHIS
- That records are kept of all contacts and communications between the CHIS and the Council/ relevant officer at the Council.

Due to the statutory requirements that need to be adhered to when using a CHIS, it is unlikely that an investigation could involve the use of a CHIS without a lot of prior planning. Assistance may be sought from the Police.

3.2 Juvenile CHIS

Special safeguards apply to the granting of authorisations where the CHIS would be a juvenile (under 18 years of age). Authorisations cannot be granted unless the provisions within The Regulation of Investigatory Powers (Juveniles) Order 2000 are satisfied.

Only the Head of Paid Service can authorise the use of a juvenile CHIS, a vulnerable CHIS and/or the acquisition of confidential information.

If any Council officer intends to use a juvenile CHIS, a vulnerable CHIS or acquire confidential information, advice and guidance should be sought from legal services before any steps are taken.

4. Communications Data

Communications data includes information relating to the use of a postal service/ telecommunications system. It does not include the contents of the communication itself. Examples of communications data include equipment and location details, telephone subscriber details, and itemised telephone bill logs.

A Single Point of Contact (SPOC) is needed to access communications data. The Council does not itself have a SPOC, although the Council is able to access the services of a SPOC. *The Council currently uses the National Anti-Fraud Network for SPOC services*. As with the other RIPA authorisations discussed above, applications will need to consider necessity, proportionality and unwanted collateral intrusion.

If you wish to access communications data, you should contact Legal Services for further information.

If there is an alternative legal power which enables a Council department to acquire communications data, this should be considered. For example, Housing Benefit Officers may wish to use the Social Security Fraud Act.

5. The lifecycle of any authorisation

Once an authorisation has been granted, the officer will need to consider the duration of the authorisation, renewal of the authorisation and cancellation of the authorisation. All authorisations are kept on a central register in Legal Services.

Duration

Communications Data authorisations cease to have effect 1 month from the date of approval, Directed Surveillance authorisations 3 months from the date of approval, and CHIS authorisations 12 months from the date of approval. The duration of a juvenile CHIS authorisation is 1 month.

Renewals

The Authorising Officer can renew an authorisation before it expires if it is necessary for the authorisation to continue for the purpose it was originally given.

An application for renewal must not be made more than 7 working days before the authorisation is due to expire. This is to ensure that the renewal is necessary.

Authorisations may be renewed more than once provided they continue to meet the criteria.

Applications for renewals must be made on another form which again should be downloaded from the Home Office website.

Reviews

When the authorisation is granted, the Authorising Officer will determine how often reviews should take place. Reviews will consider whether the authorisation is still needed, i.e whether the surveillance should continue. Review forms can be found on the Home Office website.

Cancellations

Authorisations will be cancelled when the Authorising Officer is satisfied the criteria for authorisation is no longer met. To cancel the authorisation, the officer in charge of the investigation should complete a cancellation form (found on the Home Office website). This form should then be checked by the officer's manager, and it should then be sent to the Authorising Officer.

Officers should keep copies of all applications and authorisations, original authorisations should be sent to Legal Services. Although the central register will be monitored by Legal Services, it is ultimately the Authorising Officer's responsibility to ensure renewals and cancellations are up to date.

6. The Role of the Magistrates Court

The Protection of Freedoms Act 2012 has amended the existing RIPA legislation. The amendment provides that Magistrates will have to approve RIPA authorisations before the Council can start conducting covert surveillance.

The internal process for authorisation that is detailed within this Policy remains the same, however, before any surveillance can begin, approval of Magistrates is required. Legal Services will assist with this process *and officers should refer to Appendix E and Appendix F of this Policy.*

7. The Function of the Central Register

The Central Register of all authorisations will be regularly reviewed and updated whenever an authorisation is granted, renewed or cancelled. This record should be made available to the relevant Commissioner or Inspector from the Office of Surveillance Commissioners upon request

The records should contain the following information:

- The type of authorisation
- The date the authorisation was given
- Name and rank of Authorising Officer
- The Unique Reference Number of the investigation
- The title of the investigation, including a brief description and names of subjects
- If the authorisation is renewed, when it was renewed, and who authorised the renewal
- The date the authorisation was cancelled

All investigating officers should keep a copy of the authorisation within their own department.

The Central Register will be held within the Legal Department and records will be kept for 5 years from the ending of the authorisation.

8. Exception to the need for a RIPA Authorisation

There is a limited ability in section 26(2) (c) for officers to carry out surveillance without an authorisation. If the surveillance is “an immediate response to events or circumstances”, which are unforeseen and mean that there is not sufficient time to obtain an authorisation, some degree of surveillance can be done. This may happen, for example, where the subject of an investigation is suddenly and unexpectedly observed (not during the course of surveillance) and the officer

feels vital evidence would be gained by surveilling them. This ability is restricted however, and surveillance cannot be carried on for a prolonged period of time when it would be reasonable to expect an authorisation to be sought.

9. CCTV Procedure

Use of Council owned or operated CCTV cameras to target a specific individual, individual's property or building would be directed surveillance and before such surveillance could be undertaken, a RIPA authorisation is required. When any such directed surveillance is required by a Council employee or other individual undertaking work controlled by, or on behalf of, the Council then RIPA authorisation should be pursued following the procedure detailed in paragraph 2.1 of this document. The only exception would be where an emergency situation existed and there were good reasons why an emergency RIPA application could not be made. The reasons for the operation and its emergency nature should be noted by the CCTV operator and a RIPA application made as soon as is practical.

Where the use of Council owned or operated CCTV cameras to target a specific individual, individual's property or building is requested by an external agency or organisation, it is for that agency or organisation to obtain their own RIPA authorisation. A copy of this RIPA authorisation must be passed to the appropriate responsible Council officer before any such targeted surveillance could be undertaken. If in the judgement of the CCTV operator the request is urgent, i.e. any delay would jeopardise the operation, they can authorise the use of the relevant Council's CCTV cameras but only upon receiving a written assurance from an officer of the agency or organisation that authorisation has or will be obtained. Details of the request should then be recorded by the operative and a copy of the authorisation sought as soon as is reasonably practicable. Copies of RIPA authorisations received from external agencies or organisations must be retained by the Council department which has ownership of the CCTV Camera.

10.The role of the Senior Responsible Officer, the RIPA Co-ordinator, Authorising Officers and Elected Members

The Home Office Codes of Practice say councils should appoint a Senior Responsible Officer. This person is responsible for the integrity of the surveillance process, ensuring the Council complies with RIPA and relevant legislation, and also engaging with the Inspectors when they conduct their inspections.

North Lincolnshire Council's Senior Responsible Officer is Becky McIntyre, Director of Governance and Partnerships. The responsibilities of this role are to oversee the integrity of the RIPA process, exercise oversight of the authorisations, ensure Authorising Officers are properly trained, meet with officers from the Office of Surveillance Commissioners, and implement recommendations from Inspection Reports.

North Lincolnshire Council's RIPA Co-ordinator is Lisa Langdon, Group Manager, Contentious Legal Practice. The responsibilities of this role are to keep the Central Record, exercise oversight on authorisations, organise and conduct training, and raise awareness within the Council. A proportionate and pragmatic approach will be taken to training requirements.

The Authorising Officers within the Council are Lisa Swainston Assistant Director Public Protection, and Nina Torr Assistant Director Resources and Performance. The role of the Authorising Officer is to ensure authorisations meet the requirements provided for in the legislation. The Authorising Officer's approval is the final stage within the Council's internal process. The application will then proceed to the Magistrates Court.

The Codes of Practice also say elected members should review the Council's use of RIPA and set the policy once a year. In addition to this, internal reports

on the use of RIPA should be considered to ensure RIPA is being used consistently and in accordance with the Policy. These reports are submitted to the Cabinet Member for Corporate Services and also to Lead Members.

11.Social Media

Reviewing open source sites (sites that are publicly available) does not require authorisation unless the review is carried out with some regularity, usually when creating a profile. Should a Council Officer view a site regularly or create a profile, than a directed surveillance authorisation will be required. If it becomes necessary to breach privacy and become, for example, a "friend" on the Facebook site, with the investigating officer using a false account which conceals his/her identity as a Council Officer for the purposes of obtaining intelligence, this is a covert operation and should be authorised. At the minimum, this should be authorised with a Directed Surveillance authorisation. If the investigator engages in any form of relationship with the account operator, then s/he becomes a CHIS requiring authorisation as such, and will need managing by a Controller and Handler. A record will need to be kept and a risk assessment created.

12. The role of the Investigatory Powers Commissioner's Office (IPCO)

The IPCO acts as the regulatory body in respect of RIPA. It is this office that conducts inspections of local authorities to ensure they are compliant with RIPA.

The current procedures and guidance document is **Appendix D.** This document is available from Legal Services.