Borough Council of
King's Lynn &
West Norfolk

REGULATION OF INVESTIGATORY POWERS ACT 2000 (RIPA)

POLICY

Contents

Part A Introduction & RIPA General

1. Introduction

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

1.2 All surveillance activity can pose a risk to the Borough Council of King's Lynn & West Norfolk (the Council) from challenges under the Human Rights Act 1998 (HRA) or other processes. Therefore, it must be stressed that all staff involved in the process must take their responsibilities seriously which will assist with the integrity of the Council's processes, procedures and oversight responsibilities.

1.3 In preparing this policy the Council has followed the RIPA Codes of Practice (August 2018).

1.4 The Council takes its statutory responsibilities seriously and will act in accordance with the law and the codes of practice.

2. Scope and Aim of the Policy

2.1 This policy applies to all areas of the Council and the Council's Local Authority Trading Companies (LATCs). It should be noted that where RIPA applies the law should be followed.

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

2.3 The policy also provides guidance on surveillance which it is necessary to undertake by the authority but cannot be authorised under the RIPA legislation. This is referred to as surveillance outside of RIPA and will have to be compliant with the Human Rights Act. (See section 3).

2.4 All RIPA covert activity will have to be authorised and conducted in accordance with this policy, the RIPA legislation and Codes of Practice. Therefore, all officers involved in the process will have regard to this document and the statutory RIPA Codes of Practice issued under section 71 RIPA (current version issued in August 2018) for both Directed Surveillance and the use of Covert Human Intelligence Sources (CHIS). The Codes of Practice are available from: https://www.gov.uk/government/collections/ripa-codes#current-codes-of-practice

3. Background to RIPA and Lawful Criteria

3.1 The Human Rights Act 1998 (HRA) makes it potentially unlawful for a Local Authority to breach any article of the European Convention on Human Rights (ECHR).

3.2 Article 8 of the European Convention on Human Rights states that: -

1) Everyone has the right of 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 in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health and morals or for the protection of the rights and freedoms of others.

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

3.4 Those who undertake Directed Surveillance or CHIS activity on behalf of a Local Authority may breach an individual's Human Rights, unless such surveillance is **lawful,** consistent with Article 8 of the ECHR and is both **necessary** and **proportionate** to the matter being investigated.

3.5 RIPA provides the legal framework for lawful interference to ensure that any activity undertaken, together with the information obtained, is HRA compatible.

4. Consequences of Not Following RIPA

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

- Evidence that is gathered may be inadmissible in court;
- The subjects of surveillance can bring their own claim on Human Rights grounds i.e. the Council have infringed their rights under Article 8;
- If a challenge under Article 8 is successful, the Council would receive reputational damage and could face a claim for financial compensation;
- The Government has also introduced a system of tribunal to deal with complaints. Any person who believes that their rights have been breached can have their complaint dealt with by the Investigatory Powers Tribunal (IPTC)
- It is likely that the activity could be construed as an error and therefore have to be investigated and a report submitted by the Senior Responsible Officer to the Investigatory Powers Commissioner's Office (IPCO).

5. Independent Oversight

5.1 RIPA is overseen by the Investigatory Powers Commissioner's Office (IPCO). Their remit includes providing comprehensive oversight of the use of the powers to which the RIPA code applies, and adherence to the practices and processes described in it. They also provide guidance to be followed which is separate to the codes. To carry out their full functions and duties and they will periodically inspect the records and procedures of the Council to ensure any authorisations have been given, reviewed, cancelled, and recorded properly. Therefore, it is important that the Council can show it complies with this Policy and with the provisions of RIPA.

5.2 The Codes of Practice require that as a local authority, the Council must report the fact of its use to elected council members. Members must be updated on a regular basis of any usage, or not, of the relevant powers. The Council will report its use, or

non-use of these powers to the Corporate Performance Panel in line with the guidance provided by IPCO to enable members to determine the effectiveness of the RIPA policy each year.

6. Training and Awareness

6.1 The Council recognises that an important aspect of its RIPA policy and associated procedures is the general awareness and responsiveness of employees throughout the Council. A list of key departments will be maintained by the RIPA Co-Ordinator to determine the training requirements of the Council for RIPA purposes.

Part B. Surveillance, Types and Criteria

7. Surveillance Definition

7.1 There are different types of surveillance covered by RIPA and the HRA. Surveillance can be both overt and covert and depending on their nature, are either allowed to be authorised under RIPA or not. There are also different degrees of authorisation depending on the circumstances.

7.2 **Surveillance is:**

- Monitoring, observing or listening to persons, their movements, their conversations or their other activities or communications.

- Recording anything monitored, observed or listened to in the course of surveillance, with or without the assistance of a device.

8. Overt and Covert Surveillance

8.1 Overt surveillance is where the subject of surveillance is aware that it is taking place, either by way of signage such as in the use of Closed-Circuit Television (CCTV) or because the person subject of the surveillance has been informed of the activity. Overt surveillance is outside the scope of RIPA and therefore does not require authorisation. However, it still must take account of privacy under the Human Rights Act and be necessary and proportionate. Any personal data obtained will also be subject of the Data Protection Act. Overt CCTV cameras (fixed or portable) are also subject to both the Information Commissioners and Surveillance Camera codes of practice.

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

9. Intrusive Surveillance

9.1 The Council has no authority in law to carry out Intrusive Surveillance. It is only the Police and other law enforcement agencies that can lawfully carry out intrusive surveillance.

9.2 Intrusive surveillance is defined in section 26(3) of the 2000 RIPA Act as covert surveillance that:

- Is carried out in relation to anything taking place on any residential premises or in any private vehicle; and

- Involves the presence of an individual on the premises or in the vehicle or is carried out by means of a surveillance device.

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

10. Directed Surveillance Definition

10.1 The Council can lawfully carry out Directed Surveillance. Surveillance is Directed Surveillance if the following are all true:

- It is covert, but not intrusive surveillance;

- It is conducted for the purposes of a specific investigation or operation;

- It is likely to result in the obtaining of private information (see private information below) about a person (whether or not one specifically identified for the purposes of the investigation or operation);

- It is conducted otherwise than by way of an immediate response to events or circumstances the nature of which is such that it would not be reasonably practicable for an authorisation to be sought.

11. Private information

11.1 By its very nature, surveillance may involve invading an individual's right to privacy. The Code of Practice provides guidance on what is private information. They state private information includes any information relating to a person's private or family life. As a result, private information is capable of including any aspect of a person's private or personal relationship with others, such as family and professional or business relationships.

11.2 Whilst a person may have a reduced expectation of privacy when in a public place, covert surveillance of that person's activities in public may still result in the obtaining of private information. This is likely to be the case where that person has a reasonable expectation of privacy even though acting in public and where a record is being made by a Public Authority of that person's activities for future consideration or analysis. Surveillance of publicly accessible areas of the internet should be treated in a similar way, recognising that there may be an expectation of privacy over information which is on the internet, particularly where accessing information on social media websites.

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

11.4 There is also an assessment to be made regarding the risk of obtaining collateral intrusion which relates to private information about persons who are not subjects of the surveillance This has a direct bearing when considering proportionality as part of the authorisation process.

12. Confidential or Privileged Material

12.1 This includes where the material contains information that is legally privileged, confidential journalistic material or where material identifies a journalist's source, where material contains confidential personal information or communications between a Member of Parliament and another person on constituency business. Directed Surveillance likely or intended to result in the acquisition of knowledge of confidential or privileged material must be authorised by the Chief Executive.

13. Lawful Grounds

13.1 The Lawful Grounds for Directed Surveillance is a higher threshold for Local Authorities and cannot be granted unless it is to be carried out for the purpose of preventing or detecting a criminal offence(s) and includes actions taken to avert, end or disrupt the commission of criminal offences. It must also meet the serious crime test i.e. that the criminal offence(s) which is sought to be prevented or detected is:

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

2) Would constitute an offence under sections 146, 147 or 147A of the Licensing Act 2003 or section 7 of the Children and Young Persons Act 1933 (see 1.4 above). This is the only ground available to the Council and hence the only justification.

13.2 Furthermore, the Council's authorisation can only take effect once an order approving the authorisation has been granted by a Magistrate.

13.3 RIPA ensures that any surveillance which is undertaken following authorisation and approval from a Magistrate is lawful. Therefore, it protects the authority from legal challenge. It also renders evidence obtained lawful for all purposes.

14. Urgent cases

14.1 There is no provision to authorise urgent oral authorisations under RIPA for urgent cases as all authorisations have to be approved by a Magistrate. If surveillance was required to be carried out in an urgent situation or as an immediate response, this would still have to be justified as necessary and proportionate under HRA. This type of surveillance is surveillance outside of RIPA. (see section 17 below).

15. CCTV and ANPR

15.1 The definition of CCTV is included as 'Surveillance Camera Systems' under Section 29(6) Protection of Freedoms Act 2012. "Surveillance camera systems" is taken to include:

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

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

(c) any systems for storing, receiving, transmitting, processing or checking the images or information obtained by (a) or (b);

(d) any other systems associated with, or otherwise connected with (a), (b) or

This includes

- Conventional town centre CCTV;
- Body Worn Video (BWV)
- Automatic Number Plate Recognition (ANPR);
- Deployable mobile overt mobile camera systems.
- Drones

15.2 Surveillance camera systems are subject to both the Surveillance Camera Code of Practice and the Information Commissioner's Office (ICO) CCTV Code of Practice titled 'In the Picture'

15.3 The use of the conventional town centre CCTV systems and other overt cameras operated by the Council do not normally fall under the RIPA regulations. However, should there be a requirement for the CCTV cameras to be used for a specific purpose to conduct surveillance it is likely that the activity will fall under Directed Surveillance and therefore require an authorisation.

15.4 Operators of any of the Councils CCTV system need to be aware of the RIPA issues associated with using CCTV and other camera systems and that continued, prolonged systematic surveillance of an individual may require an authorisation.

15.5 On the occasions when the CCTV cameras are to be used in a Directed Surveillance situation either by enforcement officers from relevant departments within the Council or outside Law Enforcement Agencies such as the Police, the Council's own CCTV Code of Practice should be followed where relevant as well as the RIPA Codes of Practice.

15.6 The same principles apply to Automated Number Plate Recognition (ANPR). Its use does not engage RIPA if it is used for the purpose it is registered for, such as traffic flow management or safety and enforcement within car parks. However, if used in a pre-planned way to carry out covert surveillance which meets the RIPA criteria, this policy and the codes of practice must be followed.

15.7 Where the Council are requested to assist through the facilitation of CCTV by another authority / organisation, the Council retains the right to refuse such requests should either of the following factors be absent:

- the authorised application must be completed by the authority / organisation requesting assistance through the facilitation of CCTV and;
- MUST state council officers are authorised to undertake the activities required

16. Internet and Social Media Investigations

16.1 The use of the internet and social media is constantly evolving and with it the risks associated with these types of enquiries, particularly regarding breaches of privacy under Article 8 of HRA and other operational risks. Online open-source and social media research may breach someone's privacy. It may also meet the RIPA criteria

and require authorising as per this policy. Staff are to have regards to the privacy and RIPA issues detailed in the codes of practice and advice from IPCO.

16.2 There is a separate corporate Code of Practice that covers online open source research which should be read and followed in conjunction with this policy.

17. Surveillance Outside of RIPA

17.1 As already explained, for Directed Surveillance the criminal offence must carry **a 6-month prison sentence** (Directed Surveillance crime threshold) or relate to the sale of alcohol or tobacco to children. This means that there are scenarios within an investigation that do not meet this threshold, however it is necessary to undertake surveillance. This will fall outside of RIPA. Examples include:

- Surveillance for anti-social behaviour disorder which do not attract a maximum custodial sentence of at least six months imprisonment.
- Planning enforcement prior to the serving of a notice or to establish whether a notice has been breached.
- Most licensing breaches.
- Safeguarding vulnerable people.
- Civil matters.
- Disciplinary surveillance

17.2 In the above scenarios they are likely to be a targeted surveillance which are likely to breach someone's article 8 rights to privacy. Therefore, the activity should be conducted in a way which is HRA compliant, which will include it being necessary and proportionate.

17.3 As part of the process of formally recording and monitoring non RIPA surveillance, non RIPA surveillance forms are available with the application and authorisation process being the same as for RIPA except it will not require to be approved by a Magistrate.

17.4 The Senior Responsible Officer (SRO) will maintain oversight of non RIPA surveillance to ensure that such surveillance is compliant with Human Rights legislation.

18. Joint Agency and Third-Party Surveillance

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

18.2 In some circumstances it may be appropriate or necessary for the Council to work with third parties who are not themselves a Public Authority (such as an individual, company or non-governmental organisation) to assist with an investigation. Where that third party is acting in partnership with or under the direction of the Council, then they are acting as an agent to the Council and will be subject to RIPA in the same way as any employee of the Council would be.

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

Part C. Covert Human Intelligence Sources (CHIS)

19 Introduction

19.1 RIPA covers the activities of Covert Human Intelligence Sources (CHIS) which relates not only to sources commonly known as informants (members of the public providing the Council with information), but also the activities of undercover officers. It matters not whether they are employees of the Council, agents or members of the public engaged by the Council to establish or maintain a covert relationship with someone to obtain information.

19.2 The **lawful grounds** for CHIS authorisation is prevention and detection of crime and prevention of disorder. The serious crime criteria of the offence carrying a 6-month sentence etc. does not apply to CHIS.

19.3 Recognising when a source becomes a CHIS is therefore important as this type of activity may need authorisation. Should a CHIS authority be required, all of the staff involved in the process should make themselves fully aware of the contents of this Policy and the CHIS codes of Practice.

20. Definition of CHIS

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

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

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

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

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

20.3 It is possible, that a person will become engaged in the conduct of a CHIS without a public authority inducing, asking, or assisting the person to engage in that conduct. An authorisation should be considered, for example, where a public authority is aware that a third party is independently maintaining a relationship (i.e. “self-tasking”) in order to obtain evidence of criminal activity, and the public authority intends to make use of that material for its own investigative purposes. (Section 2.26 Codes of CHIS Codes of Practice).

21. Vulnerable and Juvenile CHIS

21.1 Special consideration must be given to the use of a Vulnerable Individual as a CHIS. A ‘Vulnerable Individual’ is a person who is or may be in need of community care services by reason of mental or other disability, age or illness and who is or may be unable to take care of himself, or unable to protect himself against significant harm or exploitation. Any individual of this description, or a Juvenile as defined below, should

only be authorised to act as a source in the most exceptional circumstances and only then when authorised by the Chief Executive (or, in their absence, the Director acting up as the Chief Executive).

21.2 Special safeguards also apply to the use or conduct of Juvenile Sources; that is sources under the age of 18 years. On no occasion should the use or conduct of a source under 16 years of age be authorised to give information against his parents or any person who has parental responsibility for him. Authorisations should not be granted in respect of a Juvenile CHIS unless the special provisions contained within the Regulation of Investigatory Powers (Juveniles) Order 2000; SI No. 2793 are satisfied.

22. Risk Assessments

22.1 The Council has a responsibility for the safety and welfare of the source and as detailed in the codes of practice a risk assessment will be conducted and all the guidance contained within the codes will be followed.

Part D. Roles and Responsibilities

23 The Senior Responsible Officer (SRO)

23.1 The nominated Senior Responsible Officer is the Chief Executive (see Appendix A) The SRO with responsibilities for:

- The integrity of the process in place within the Council to authorise Directed and Intrusive Surveillance;
- Compliance with the relevant sections of RIPA and the Codes of Practice;
- Oversight of the reporting of errors to the Investigatory Powers Commissioner (IPC) and the identification of both the cause(s) of errors and the implementation of processes to minimise repetition of errors;
- Engagement with the Investigatory Powers Commissioner Office (IPCO) and the inspectors who support the Commissioner when they conduct their inspections;
- Where necessary, overseeing the implementation of any recommended post-inspection action plans and
- Ensuring that all Authorising Officers are of an appropriate standard, addressing any recommendations and concerns in the inspection reports prepared by the Investigatory Powers Commissioner.

24. RIPA Co-Ordinator

24.1 The RIPA Co-Ordinator (see appendix A) is responsible for storing all the original authorisations, reviews, renewals and cancellation forms and the signed approval or refusal documentation from the Magistrate. This will include any authorisations that have not been authorised by the Authorising Officer or refused by a Magistrate.

24.2 The RIPA Co-ordinator will: -

- Keep the copies of the forms for a period of at least 5 years;

- Keep the Central Register (a requirement of the Codes of Practice) of all authorisations, renewals and cancellations; and issue the unique reference number. This will also identify and monitor expiry and renewal dates.

- Must ensure that any electronic and paper records relating to a RIPA investigation are used, retained or destroyed in line with the Councils Information Management policies, departmental retention schedules and the Data Protection Act 2018. (DPA)

- Provide administrative support and guidance on the processes involved.

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

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

- Provide or identify training and further guidance and awareness of RIPA and the provisions of this Policy; and Review the contents of this Policy.

25. Authorising Officers

25.1 The Regulation of Investigatory Powers (Directed Surveillance and Covert Human Intelligence Sources) Order 2010 prescribes that for Local Authorities the Authorising Officer shall be a Director, Head of Service, Service Manager or equivalent as distinct from the officer responsible for the conduct of an investigation. Authorising Officers within the Council who can grant authorisations all of which are at Assistant Director level or above and have received the appropriate training. (see appendix A).

25.2 Authorising Officers should not be responsible for authorising investigations or operations in which they are directly involved. The role of the Authorising Officers is to consider whether to authorise, review, or renew an authorisation. They must also officially cancel the RIPA covert activity. Authorising Officers must have been trained to an appropriate level to have an understanding of the requirements in the Codes of Practice and that must be satisfied before an authorisation can be granted.

26 Necessity and Proportionality

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

26.2 The Authorising Officer must believe that the authorisation is necessary in the circumstances of the particular case for one or more of the statutory grounds which for Local Authority Directed Surveillance is the prevention and detection of crime and that the crime attracts a custodial sentence of a maximum of 6 months or more, or for the purpose of preventing or detecting specified criminal offences relating to the underage sale of alcohol and tobacco.

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

26.4 The applicant and Authorising Officers must also be able to demonstrate why it is necessary to carry out the covert activity to achieve the objectives and that there were no other means of obtaining the same information in a less intrusive method. This is a part of the authorisation form.

26.5 If the activities are deemed necessary, the Authorising Officer must also believe that they are **proportionate** to what is sought to be achieved by carrying them out. This involves balancing the seriousness of the intrusion into the privacy of the subject of the operation (or any other person who may be affected) against the need for the activity in investigative and operational terms. The authorisation will not be proportionate if it is excessive in the overall circumstances of the case.

27. Collateral Intrusion

27.1 The Authorising Officer should also take into account the risk of obtaining collateral intrusion which is private information about persons who are not subjects of the surveillance. Staff should take measures, wherever practicable, to avoid or minimise unnecessary intrusion into the privacy of those who are not the intended subjects of the surveillance.

28 Forms and Durations

28.1 For both Directed Surveillance and CHIS authorisations there are the forms within the process. They are:

- Authorisation
- Review
- Renewal
- Cancellation
- Magistrates Form

28.2 Authorisations must be given for the maximum duration from the Date approved by the Magistrate but reviewed on a regular basis and formally cancelled when no longer needed. They do not expire, they must be cancelled when the surveillance is no longer proportionate or necessary. No surveillance etc. can be undertaken after the expiry date unless renewed and approved by the Magistrate. Durations detailed below:

• Directed Surveillance	3 Months
• Renewal	3 Months
• Covert Human Intelligence Source	12 Months
• Renewal	12 months
• Juvenile Sources	4 Months
• Renewal	4 Months

28.3 These durations also apply to any surveillance activities undertaken outside of RIPA.

Part E Central Record and Safeguarding the Material

29. Central Record

29.1 The council will maintain a centrally retrievable record of all authorisations/refusals to authorise will be held and maintained by RIPA Co-Ordinator. It will be regularly updated whenever an authorisation is applied for, refused, granted, renewed or

cancelled. The record will be made available to the relevant Commissioner or an Inspector from IPCO, upon request.

29.2 The documents contained in the centrally held register should be retained for at least three years from the ending of the authorisation or for the period stipulated by the Council's document retention policy, whichever is greater. The centrally held register contains the following information:

- If refused, (the application was not authorised by the AO) a brief explanation of the reason why. The refused application should be retained as part of the central record of authorisation;
- If granted, the type of authorisation and the date the authorisation was given;
- Details of attendances at the magistrates' court to include the date of attendances at court, the determining magistrate, the decision of the court and the time and date of that decision;
- Name and grade of the authorising officer;
- The unique reference number (URN) of the investigation or operation;
- The title of the investigation or operation, including a brief description and names of subjects, if known;
- Frequency and the result of each review of the authorisation;
- If the authorisation is renewed, when it was renewed and who authorised the renewal, including the name and grade of the authorising officer and the date renewed by the Magistrate;
- Whether the investigation or operation is likely to result in obtaining confidential information as defined in this code of practice;
- The date the authorisation was cancelled;
- Authorisations by an Authorising Officer where they are directly involved in the investigation or operation. If this has taken place it must be brought to the attention of a Commissioner or Inspector during their next RIPA inspection.

29.3 As well as the central record the Council will also retain:

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

- The date and time when any instruction to cease surveillance was given;
- The date and time when any other instruction was given by the Authorising Officer;
- A record of the period over which the surveillance has taken place. This should have been included within the cancellation form. Decide on the cancellation form to be used.

29.4 Detailed records must be kept of the authorisation and the use made of a CHIS. The Regulation of Investigatory Powers (Source Records) Regulations 2000; SI No: 2725 details the particulars that must be included in these records. The council will comply with these requirements.

30. Safeguarding the Use of Surveillance and CHIS Material

30.1 This section provides guidance on the procedures and safeguards to be applied in relation to the handling of any material obtained through Directed Surveillance or CHIS activity. This material may include private, confidential, or legal privilege information. It will also show the link to other relevant legislation.

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

31. Authorised Purpose

31.1 Dissemination, copying and retention of material must be limited to the minimum necessary for an **authorised purposes**. Something is necessary for the authorised purposes if the material:

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

32. Use of Material as Evidence

32.1 Material obtained through Directed Surveillance, may be used as evidence in criminal proceedings. The admissibility of evidence is governed primarily by the common law, the Criminal Procedure and Investigations Act 1996 (CPIA), the Civil Procedure Rules, section 78 of the Police and Criminal Evidence Act 1984 and the Human Rights Act 1998.

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

33. Dissemination of Information

33.1 It may be necessary to disseminate material acquired through the RIPA covert activity. The number of persons to whom any of the information is disclosed, and the extent of disclosure, should be limited to the minimum necessary. It must also be in connection with an authorised purpose as set out in section 31 above. It will be necessary to consider exactly what and how much information should be disclosed. Only so much of the material may be disclosed as the recipient needs; for example, if a summary of the material will suffice, no more than that should be disclosed.

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

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

34. Storage, Copying and Destruction

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

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

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

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

Part F Errors and Complaints

35. Errors

35.1 Errors relating to the RIPA process can have consequences to an affected individual's rights. Proper application of the surveillance and CHIS provisions in the RIPA codes and this Policy should reduce the scope for making errors. There is a process detailed within the codes of practice relating to errors.

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

- Relevant error and
- Serious error.

Examples of relevant errors would include circumstances where:

- Surveillance activity has taken place without lawful authorisation.
- There has been a failure to adhere to the safeguards set out in the relevant statutory provisions and Chapter 9 of the Surveillance Codes of Practice relating to the safeguards of the material.

35.2 The Council will comply with the procedures set out in the codes by establishing whether the error is a relevant error and if so it will be reported to IPCO who will determine whether it is a serious error and what action to take. A serious error is one that has caused significant prejudice or harm to the person concerned.

36 Complaints

36.1 Any person who reasonably believes they have been adversely affected by surveillance activity by or on behalf of the Council may complain:

- online within the "Have your say" webpage on the Council's website (www.west-norfolk.gov.uk)
- By calling the Council information Centre on 01553 616200
- By email to complaints@west-norfolk.gov.uk
- In person at our Council Offices, or
- By writing to Complaints, Democratic Services Department, Borough Council of King's Lynn & West Norfolk, Kings Court, Chapel Street, King's Lynn, PE30 1EX

36.2 A complaint can also be made to the official body which is the Investigatory Powers Tribunal (IPT). They have jurisdiction to investigate and determine complaints against any Public Authority's use of RIPA powers, including those covered by this Policy.

Complaints should be addressed to:

The Investigatory Powers Tribunal

PO Box 33220

London

SWIH 9ZQ

37 Version Control

Policy name		Regulation of Investigatory Powers Act 2000 (RIPA) Policy
Policy description		To ensure that the Borough Council of King's Lynn and West Norfolk (the Council) and its officers when undertaking covert investigative activities which may interfere with a

		person's right to respect for private and family life, home and correspondence, do so in such a way that is compatible with the European Convention on Human Rights (ECHR), the Human Rights Act 1998 (HRA), the Regulation of Investigatory Powers Act 2000 (RIPA), the Protection of Freedoms Act 2012, the Investigatory Powers Act 2016 (IPA), the General Data Protection Regulations (GDPR) and the Data Protection Act 2018 (DPA).		
Responsible Officer		Lorraine Gore, Chief Executive		
Version number	Date formally approved	Reason for update	Author	Review date
1.0		To consider changes in the law and also guidance and details identified through inspections by IPCO.	Jamie Hay / Mark Whitmore / Paul Fowler (Consultant)	April 2025