NORTH NORFOLK DISTRICT COUNCIL

THE REGULATION OF INVESTIGATORY POWERS ACT 2000 POLICY AND PROCEDURES

Updated September 2021

This page left intentionally blank

NORTH NORFOLK DISTRICT COUNCIL

REGULATION OF INVESTIGATORY POWERS ACT 2000 ("RIPA")

POLICY DOCUMENT

1. INTRODUCTION

This Act has significant implications for many areas of work carried out by the Council. The Act does not in any way restrict its operation to specific functions and therefore it is imperative that any officer who might be carrying out surveillance and Authorising Officers are fully aware of when the need arises for an authorisation to be obtained. This document only sets out the main principles involved around covert surveillance. It must be stressed that any officer requesting authorisation and particularly those persons empowered by the Council to grant authorisations must ensure they receive full and proper training before dealing with any authorisations. However, a considerable amount of what the Council does is COVERT so that the person being investigated is fully aware of the situation. This will never need authorisation.

The information contained within this document has been extracted from the two relevant **Codes of Practice** issued pursuant to section 71 of RIPA 2000, namely the **Covert Surveillance Code (Surveillance Code)** and the **Covert Human Intelligence Sources Code (CHIS Code)**, and guidance produced by the Office of Surveillance Commissioners (IPCO) who are the independent inspectors.

There are two types of covert surveillance which might arise in local government, operations, **Directed Surveillance** and **Covert Human Intelligence Sources** (CHIS) (ie informants, undercover officers, test purchase officers) which are further explained later in this document.

A third type, **Intrusive Surveillance**, cannot be authorised by local authorities (see section 8).

Note: Directed surveillance does not include entry on, or interference with, property or wireless telegraphy, nor does it include interception of communications sent by post or by telecommunication systems. These can only be carried out by the Secretary of State, Police or intelligence agencies (depending upon the situation). However, you should not rule out directed surveillance simply because you might overhear telephone conversations, but you cannot deliberately place a device so as to hear such conversations.

2. CONSEQUENCES OF FAILURE TO COMPLY WITH THE LEGISLATION

Article 8 of the Human Rights Convention introduced a new concept in English Law, the right to privacy which is a qualified right. To comply with this human right, surveillance, which potentially infringes the right to privacy, should only be done if it is carried out "in accordance with the law" and is necessary and proportionate. Hence a legal framework to authorise surveillance was required and RIPA was introduced.

RIPA Authorisation provides a lawful authority to carry out covert surveillance provided it is authorised in accordance with the Act. However, a decision not to obtain authorisation does not automatically render the surveillance unlawful. The Act and Codes of Practice are admissible in evidence and so whether authorisation was correctly obtained will be taken into account in any court proceedings about admissibility of evidence and/or human rights challenges. If the Council fails to comply with RIPA it could be ordered to pay compensation either by a court or the ombudsman. An innocent party to collateral intrusion could be entitled to a considerable amount of compensation. It is also possible that evidence gathered via unauthorised surveillance could be ruled inadmissible. This policy document recommends that authorisations are always obtained in accordance with the Act, where appropriate.

The Senior Responsible Officer

In accordance with the Code of Practice each public authority must have a Senior Responsible Officer who is responsible for:

- The integrity of the process in places within the public authority to acquire communications data;

- Compliance with Chapter II of Part 1 of RIPA and with the Code;

- Oversight of the reporting of errors to the Interception of Communications Commissioner's Office (IOCCO) and the identification of both the cause of errors and the implementation of processes to minimise repetition of errors;

- Engagement with the IOCCO inspectors when they conduct their inspections and;

- Where necessary, oversee the implementation of post – inspection action plans approved by the Commissioner

3. INVESTIGATORY POWERS COMMISSIONER'S OFFICE (IPCO)

The legislation provides for an Investigatory Powers Commissioner, whose remit it is to provide an independent oversight of the use of the powers contained within Part 2 of the Act, by public authorities.

The IPCO will periodically visit the Council for an inspection of our records and protocol. The aims of any inspections are to be as helpful as possible providing feedback on best practice, recurring problem areas and remedies.

4. PROTECTION OF FREEDOMS ACT 2012

Judicial approval

The Act amends RIPA, requiring local authorities to obtain the approval of a Magistrate for the use of any one of the three covert investigatory techniques available to them under RIPA namely:

- Directed Surveillance,

- Deployment of a Covert Human Intelligence Source (CHIS)

An approval is also required if an authorisation to use such techniques is being renewed. In each case, the role of the Magistrate is to ensure that the correct procedures have been followed and the relevant factors have been taken account of. The new provisions allow the Magistrate, on refusing an approval of an authorisation, to quash that authorisation.

Directed Surveillance and the Serious Crime Test

Where local authorities wish to use RIPA to authorise Directed Surveillance, this must be confined to cases where the offence under investigation carries a maximum custodial sentence of six months or more (the Serious Crime Test) or criminal offences under sections 146, 147 or 147A of the Licensing Act 2003 or section 7 of the Children and Young Persons Act 1933 relating to the sale of alcohol or tobacco products to children.

On completion of the Council's internal authorisation procedures application must be made to Her Majesty's Courts and Tribunals Service (HMCTS) administration at the magistrates' court to arrange a hearing.

Court attendance will be required with:

- a counter-signed RIPA authorisation/or notice.
- the accompanying judicial application/order form.
- any other relevant reference or supporting material.

5. SURVEILLANCE

The Definition of Surveillance includes:

(a) monitoring, observing or listening to persons, their movements, their conversations or their other activities or communications;

(b) recording anything monitored, observed or listened to in the course of surveillance; and

(c) surveillance by or with the assistance of a surveillance device.

Definition of Directed Surveillance

An authorisation is required for covert surveillance undertaken:

(a) for a specific investigation or operation; and

(b) where the surveillance is likely to result in obtaining private information about any person (whether or not they are the subject of the surveillance).

An authorisation is **NOT** required for covert surveillance carried out as an immediate response to events or circumstances, which could not be foreseen such as an enforcement officer noticing something whilst travelling around the town which requires them to observe the activities of a person(s). Equally any surveillance which is overt due to the fact the persons have been warned is not Directed Surveillance.

Directed Surveillance is defined as surveillances where 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 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 under Part II of the 2000 Act to be sought.

Thus, the planned covert surveillance of a specific person, where not intrusive, would constitute directed surveillance if such surveillance is likely to result in the obtaining of private information about that, or any other person.

6. PRIVATE INFORMATION

Private information is defined in the Codes of Practice as including any information relating to a person's private or family life. Private information should be taken generally to include any aspect of a person's private or personal relationship with others, including family and professional or business relationships.

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.

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

Directed surveillance does not include any type of covert surveillance carried out in residential properties or in private vehicles (see section below). This is Intrusive Surveillance that local authorities cannot authorise.

7. COLLATERAL INTRUSION

The officer seeking the authorisation should also consider the possibility of collateral intrusion. This is private information about persons who are not subjects of the surveillance or property interference activity. Steps should be taken to assess the risk, and where possible minimise the risk of collateral intrusion. Where unforeseen collateral intrusion occurs during an operation, the

Authorising Officer must be notified and consideration given to amending the authorisation following a review.

Consideration must also be given as to whether or not the surveillance activities of the Service take place where similar activities are also being undertaken by another agency e.g., the Police or Environment Agency etc.

If at any stage during the surveillance it becomes apparent that there is unexpected interference into the privacy of persons who are not the original subject of the investigation then this information and any other matters that arise of a similar sensitive nature, should be brought to the Authorising Officers attention. This will enable the Authorising Officer to reconsider the original authorisation taking into consideration the new information. The Authorising Officer should particularly bear in mind the proportionality of the surveillance in this situation.

8. INTRUSIVE SURVEILLANCE

Intrusive Surveillance is defined in section 26(3) of the 2000 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.

An example would be placing a listening device inside residential premises. Surveillance equipment mounted outside the premises will not be intrusive, unless the device consistently provides information of the same quality and detail as might be expected if they were in the premises/vehicle.

Local authorities cannot authorise Intrusive Surveillance.

9. EMERGENCY SITUATIONS

There is no longer any provision to obtain an urgent oral authority. Therefore, any surveillance which was urgent will be regarded as surveillance outside of the

RIPA legislation. However, the activity would still have to meet the test of Necessity and Proportionality and should be justified in writing following the activity taking place.

Other Surveillances

Similarly, the District Council cannot conduct entry on, or interference with, property or with wireless telegraphy (known as “property interference”).

Authorisation Forms and the Application Process

The below forms are to be used to comply with the process. They can be obtained from North Norfolk District Council Intranet site:

- Authorisation form (also contains the application section)
- Judicial Application/Order form
- Review form
- Renewal form
- Cancellation form

No covert activity covered by RIPA or the use of a CHIS should be undertaken at any time unless it meets the legal criteria (see above) and has been authorised by an Authorising Officer and approved by a JP/Magistrate as mentioned above. The activity conducted must be in strict accordance with the terms of the authorisation.

The effect of the above legislation means that all applications and renewals for covert RIPA activity will have to have a JP’s approval. It does not apply to Reviews and Cancellations which will still be carried out internally.

The procedure is as follows:

All applications and renewals for Directed Surveillance and use of a CHIS will be required to have a JP’s approval.

The applicant will complete the relevant application form ensuring compliance with the statutory provisions shown above. The application form will be submitted to an Authorising Officer for consideration. If authorised, the applicant will also complete the required section of the judicial application/order form. Although this form requires the applicant to provide a brief summary of the circumstances of the case on the judicial application form, this is supplementary to and does not replace the need to supply the original RIPA authorisation as well.

It will then be necessary within Office hours to arrange with Her Majesty's Courts & Tribunals Service (HMCTS) administration at the magistrates' court to arrange a hearing. The hearing will be in private and heard by a single JP.

The Authorising Officer will be expected to attend the hearing along with the applicant officer. Officers who may present the application at these proceedings will need to be formally designated by the Council under section 223 of the Local Government Act 1972 to appear, be sworn in and present evidence or provide information as required by the JP. If in doubt as to whether you are able to present the application seek advice from the Solicitor to the Council.

Upon attending the hearing, the officer must present to the JP the partially completed judicial application/order form, a copy of the RIPA application/authorisation form, together with any supporting documents setting out the case, and the original application/authorisation form.

The original RIPA application/authorisation should be shown to the JP but will be retained by the local authority so that it is available for inspection by the Commissioners' offices and in the event of any legal challenge or investigations by the Investigatory Powers Tribunal (IPT).

The JP will read and consider the RIPA application/ authorisation and the judicial application/order form. They may have questions to clarify points or require additional reassurance on particular matters. These questions are supplementary to the content of the application form. However the forms and supporting papers must by themselves make the case. It is not sufficient for the local authority to

provide oral evidence where this is not reflected or supported in the papers provided.

The JP will consider whether he or she is satisfied that at the time the authorisation was granted or renewed, there were reasonable grounds for believing that the authorisation was necessary and proportionate. They will also consider whether there continues to be reasonable grounds. In addition they must be satisfied that the person who granted the authorisation or gave the notice was an appropriate designated person within the local authority and the authorisation was made in accordance with any applicable legal restrictions, for example that the crime threshold for directed surveillance has been met.

The JP may decide to:

- Approve the Grant or renewal of an authorisation.

The grant or renewal of the RIPA authorisation will then take effect and the local authority may proceed to use the technique in that particular case. The duration of the authorisation commences with the magistrate's approval.

- Refuse to approve the grant or renewal of an authorisation

The RIPA authorisation will not take effect and the local authority may not use the technique in that case.

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

For, a technical error, the form may be remedied without going through the internal authorisation process again. The officer may then wish to reapply for judicial approval once those steps have been taken.

Refuse to approve the grant or renewal and quash the authorisation or notice

This applies where the JP refuses to approve the application/authorisation or renew the application/authorisation and decides to quash the original authorisation or notice. However the court must not exercise its power to quash the application/authorisation unless the applicant has had at least 2 business days from the date of the refusal in which to make representations. If this is the case the officer will inform the Legal section who will consider whether to make any representations.

Whatever the decision the JP will record their decision on the order section of the judicial application/order form. The court administration will retain a copy of the local authority RIPA application and authorisation form and the judicial application/order form. The officer will retain the original application/authorisation and a copy of the judicial application/order form.

If approved by the JP, the date of the approval becomes the commencement date and the three months duration will commence on this date, the officers are now allowed to undertake the activity.

The original application and the copy of the judicial application/order form should be forwarded to the Central Register and a copy retained by the applicant and if necessary by the Authorising Officer.

A local authority may only appeal a JP decision on a point of law by judicial review. If such a concern arises, the Legal team will decide what action if any should be taken.

If it is intended to undertake both directed surveillance and the use of a CHIS on the same surveillance subject, the respective applications forms and procedures should be followed and both activities should be considered separately on their own merits.

An application for an authorisation must include an assessment of the risk of any collateral intrusion or interference. The Authorising Officer will take this into

account, particularly when considering the proportionality of the directed surveillance or the use of a CHIS.

Application, Review, Renewal and Cancellation Forms

Applications

All the relevant sections on an application form must be completed with sufficient information for the Authorising Officer to consider Necessity, Proportionality and the Collateral Intrusion issues. Risk assessments should take place prior to the completion of the application form. Each application should be completed on its own merits of the case. Cutting and pasting or using template entries should not take place as this would leave the process open to challenge.

All applications will be submitted to the Authorising Officer via the Line Manager of the appropriate enforcement team in order that they are aware of the activities being undertaken by the staff. Applications whether authorised or refused will be issued with a unique number by the Authorising Officer, taken from the next available number in the Central Record of Authorisations.

If authorised the applicant will then complete the relevant section of the judicial application/order form and follow the procedure above by arranging and attending the Magistrates Court to seek a JP's approval. The duration of the authorisation commences with the magistrate's approval. (see procedure on page 10 - RIPA application and authorisation process)

Duration of Applications

Directed Surveillance	3 Months
Renewal	3 Months
Covert Human Intelligence Source	12 Months
Renewal	12 months
Juvenile Sources	1 Month

Renewal 1 Month

No authorisation can be authorised for a lesser period and the Authorising Officer should set the time and date to expire as 2359 hours on the day before the expiration of the relevant authorisation period shown above.

All Authorisations must be cancelled by completing a cancellation form at the earliest opportunity. They must not be left to simply expire.

Reviews

The reviews are dealt with internally by submitting the review form to the Authorising Officer. There is no requirement for a review form to be submitted to a JP. However, if a different surveillance technique is required it is likely a new application will have to be completed and approved by a JP.

Regular reviews of authorisations should be undertaken to assess the need for the surveillance to continue. The results of a review should be recorded on the central record of authorisations. Particular attention is drawn to the need to review authorisations frequently where the surveillance provides access to confidential information or involves collateral intrusion.

In each case the Authorising Officer should determine how often a review should take place. This should be as frequently as is considered necessary and practicable and they will record when they are to take place on the application form. This decision will be based on the circumstances of each application. However, reviews will be conducted on a monthly or less basis to ensure that the activity is managed. It will be important for the Authorising Officer to be aware of when reviews are required following an authorisation to ensure that the applicants submit the review form on time.

Applicants should submit a review form by the review date set by the Authorising Officer. They should also use a review form for changes in circumstances to the original application so that the need to continue the activity can be reassessed. However, if the circumstances or the objectives have changed considerably, or the techniques to be used are now different a new application form should be submitted and will be required to follow the process again and be approved by a

JP. The applicant does not have to wait until the review date if it is being submitted for a change in circumstances.

Managers or Team Leaders of applicants should also make themselves aware of when the reviews are required to ensure that the relevant forms are completed on time.

Renewal

Should it be necessary to renew a Directed Surveillance or CHIS application/authorisation, this must be approved by a JP.

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

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

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

If the Authorising Officer refuses to renew the application the cancellation process should be completed. If the AO authorises the renewal of the activity the same process is to be followed as mentioned earlier for the initial application.

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

Cancellation

The cancellation form is to be submitted by the applicant or another investigator in their absence. The Authorising Officer who granted or last renewed the authorisation must cancel it if they are satisfied that the directed surveillance no longer meets the criteria upon which it was authorised. Where the Authorising Officer is no longer available, this duty will fall on the person who has taken over the role of Authorising Officer or the person who is acting as Authorising Officer

As soon as the decision is taken that directed surveillance should be discontinued, the applicant or other investigating officer involved in the investigation should inform the Authorising Officer. The Authorising Officer will formally instruct the investigating officer to cease the surveillance, noting the time and date of their decision. This will be required for the cancellation form. The date and time when such an instruction was given should also be recorded in the central record of authorisations (see paragraph 5.18 in the Codes of Practice). It will also be necessary to detail the amount of time spent on the surveillance as this is required to be retained by the Senior Responsible Officer.

The officer submitting the cancellation should complete in detail the relevant sections of the form and include the period of surveillance and what if any images were obtained and any images containing third parties. The Authorising Officer should then take this into account and issues instructions regarding the management and disposal of the images etc.

The cancellation process should also be used to evaluate whether the objectives have been achieved and whether the applicant carried out what they stated was necessary in the application form. This check will form part of the oversight function. Where issues are identified they will be brought to the attention of the line manager and the Senior Responsible Officer (SRO). This will assist with future audits and oversight.

10. SENIOR RESPONSIBLE OFFICER (SRO) AND AUTHORISING OFFICERS (AO)

Senior Responsible Officer details and Officers authorised to consider authorising applications for Directed Surveillance and CHIS

SRO	Name	Contact Details
Stephen Hems	Director of Communities	01263 516182 stephen.hems@north-norfolk.gov.uk
Authorising Officers		
Emily Capps	Assistant Director for Environment and Leisure Services	01263 516274 Emily.capps@north-norfolk.gov.uk
Tracy Howard	Public Protection and Commercial Manager	01263 516139 Tracy.howard@north-norfolk.gov.uk

The SRO will ensure that sufficient numbers of AO's from each service are, after suitable training on RIPA and this document, duly certified to take action under this document.

Such authorisations are for directed surveillance or the use of covert human intelligence sources as defined in Article 4 of The Regulation of Investigatory Powers (Directed Surveillance and Covert Human Intelligence Sources) Order 2003.

Other officers may be authorised to approve applications on Directed Surveillance as deemed necessary by the NNDC Corporate Leadership Team.

Any officer authorising such decisions must ensure that he or she is properly trained so that the decision is made in accordance with the law. It is important that the person seeking authorisation and the Authorising Officer ensures that the decision to take (and it is recommended not to take) action is properly documented with full reasons. Comments should be put in the necessity and proportionality box in the application form even if these are just "I agree". It is also important to note that the Authorising Officer's job does not stop should s/he agree to authorisation. That person must keep the investigation under review, particularly if information may be obtained about someone other than the target of the surveillance (collateral intrusion). In all surveillance the risks should also be assessed properly and kept under review. So that there is a proper review system officers should record the date when the authorisation should be reviewed. Whilst this can be the full 3 months permitted the review will invariably be a much shorter period of up to 1 month.

Gatekeeper

The SRO is not the most appropriate person to undertake the responsibility of Gatekeeper and it would be anticipated that, following completion, applications would be reviewed by the NNDC Gatekeeper, Mrs Cara Jordan, who will give advice where necessary to the applicant. The form would be referred to the Authorising Officer for authorisation and if authorised, will then be submitted for Magistrate's approval.

What the Authorising Officer must take into account?

1. For Directed Surveillance, ensure that the offence meets the criteria.

2. Ensure compliance with the data protection requirements and any other relevant codes of practice and ensure that any confidential material obtained during the course of the surveillance is securely maintained. Confidential material includes matters subject to legal privilege, confidential personal information and confidential journalistic material. These terms are explained further in the Surveillance Code. Where it is likely that the surveillance will result in the acquisition of such information, the Authorising Officer will discuss with the SRO before authorisation will be given.

3. Consider the impact of **collateral intrusion** relating to persons other than the subject of the surveillance. (see explanation above).

4. **Proportionate** to what the surveillance seeks to achieve. In other words, is the Council over using its resources in order to get the result?

   The Authorising Officer must:

   a. balance the size and scope of the operation against the gravity and extent of the perceived mischief

   b. explain how and why the methods to be adopted will cause the least possible intrusion on the target and others

   c. ensure that the activity is an appropriate use of the legislation and the only reasonable way, having considered all others, of obtaining the necessary result

   d. evidence what other methods had been considered and why they were not implemented.

   The Authorising Officer should set out why he is satisfaction or why s/he believes the surveillance proposed is necessary and proportionate. A bare assertion is insufficient.

5. Special care needs to be given in relation to **joint operations** with other agencies and where the Council employs an agent to carry out investigations on its behalf.

6. Legal Advice. It is recommended that legal advice is sought from the Council's legal advisors on any proposed RIPA surveillance prior to authorisation.

Central Records

Each Authority must retain certain information relating to all authorisations, giving details of what the authorisation was for and the dates during which surveillance has been carried out. The Authorising Officer should retain a copy of relevant

documentation for their own reference; however, they must also send the original authorisation form to the SRO and RIPA Co-ordinator for filing and inclusion in the central register within 5 days.

A full list of the matters to be recorded are contained with paragraph 8.1 and 8.2 in the Covert Surveillance Code and paragraphs 7.1 to 7.7 in the Covert Human Intelligence Codes if authorising CHIS activity. This information is recorded on the Central Register.

The NNDC RIPA Coordinator and keeper of the central record of authorisations responsibilities are to collate all applications/authorisations, reviews, renewals and cancellations which are maintained in a RIPA file. In addition, they issue the appropriate forms for completion by applicants, keep the policy up-to-date, have meetings with the Authorising Officer to discuss RIPA issues, organises training and in conjunction with the Authorising Officer prepares RIPA information to Council committees.

11. COVERT HUMAN INTELLIGENCE SOURCE (CHIS)

Introduction

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.

Not all human source activity will meet the definition of a CHIS. For example, a source may be a public volunteer or someone who discloses information out of professional or statutory duty or has been tasked to obtain information other than by way of a covert relationship. However, Officers must be aware that such information may have been obtained in the course of an ongoing relationship with a family member, friend or business associate. The Council has a duty of care to all members of the public who provide information to us and appropriate measures must be taken to protect that source. How the information was

obtained should be established to determine the best course of action. The source and information should also be managed correctly in line with CPIA and the disclosure provisions.

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.

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

Legal advice should always be sought where consideration is given to the use of CHIS.

Definition of CHIS

Individuals act as a Covert Human Intelligence source (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

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.

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)

Vulnerable and Juvenile CHIS

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 one of the Directors in the Chief Executives absence.

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.

If the use of a Vulnerable Individual or a Juvenile is being considered as a CHIS you must consult the Gatekeeper before authorisation is sought as authorisations should not be granted in respect of a Juvenile CHIS unless the special provisions contained within the Regulation of Investigatory Powers (Juveniles) Order 2000; SI No. 2793 are satisfied.

Lawful Criteria

The lawful criteria 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.

Authorisations for Juvenile Sources must be authorised by the Chief Executive of the Council (or, in their absence, the Deputy Chief Executive/Directors).

Conduct and Use of a Source

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

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

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

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

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

c. Incidental to anything falling within a. and b. above.

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

The use of a source is what the Authority does in connection with the source, such as tasking and the conduct is what a source does to fulfil whatever tasks are given to them or which is incidental to it. The Use and Conduct require separate consideration before authorisation. However, they are normally authorised within the same authorisation.

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

Care should be taken to ensure that the CHIS is clear on what is or is not authorised at any given time, and that all the CHIS's activities are properly risk assessed. Care should also be taken to ensure that relevant applications,

reviews, renewals and cancellations are correctly performed. (Section 210 CHIS Codes of Practice)

Careful consideration must be given to any particular sensitivities in the local community where the CHIS is being used and of similar activities being undertaken by other public authorities which could have an impact on the deployment of the CHIS. Consideration should also be given to any adverse impact on community confidence or safety that may result from the use or conduct of a CHIS or use of information obtained from that CHIS. (Section 3.18 CHIS Codes of Practice)

Handler and Controller

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

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

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

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

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

- Dealing with the source on behalf of the Local Authority concerned;

- Risk assessments

- Directing the day to day activities of the source;

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

The **Controller** will be responsible for:

- The management and supervision of the "Handler" and
- General oversight of the use of the CHIS;
- Maintaining an audit of case work sufficient to ensure that the use or conduct of the CHIS remains within the parameters of the extant authorisation.

Undercover Officers

Oversight and management arrangements for **undercover operatives**, while following the principles of the Act, will differ, in order to reflect the specific role of such individuals as members of the Council. The role of the handler will be undertaken by a person referred to as a **'cover officer'**. (Section 6.9 CHIS Codes of Practice).

Tasking

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

In some instances, the tasking given to a person will not require the source to establish a personal or other relationship for a covert purpose. For example, a member of the public is asked to maintain a record of all vehicles arriving and leaving a specific location or to record the details of visitors to a neighbouring house. A relationship has not been established or maintained in order to gather

the information and a CHIS authorisation is therefore not available. Other authorisations under the Act, for example, Directed Surveillance, may need to be considered where there is a possible interference with the Article 8 rights of an individual.

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

Risk Assessments

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

Use of Equipment by a CHIS

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

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

CHIS Management

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

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

CHIS Record Keeping

Centrally Retrievable Record of Authorisations

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

The records are retained for 5 years from the ending of the authorisation.

Individual Source Records of Authorisation and Use of CHIS

Detailed records must be kept of the authorisation and the use made of a CHIS. An Authorising Officer must not grant an authorisation for the use or conduct of a CHIS unless they believe that there are arrangements in place for ensuring that there is at all times a person with the responsibility for maintaining a record of the use made of the CHIS. The Regulation of Investigatory Powers (Source Records)

Regulations 2000; SI No: 2725 details the particulars that must be included in these records.

The particulars to be contained within the records are;

a. The identity of the source;
b. The identity, where known, used by the source;
c. Any relevant investigating authority other than the authority maintaining the records;
d. The means by which the source is referred to within each relevant investigating authority;
e. Any other significant information connected with the security and welfare of the source;
f. Any confirmation made by a person granting or renewing an authorisation for the conduct or use of a source that the information in paragraph (d) has been considered and that any identified risks to the security and welfare of the source have where appropriate been properly explained to and understood by the source;
g. The date when, and the circumstances in which the source was recruited;
h. Identity of the Handler and Controller (and details of any changes)
i. The periods during which those persons have discharged those responsibilities;
j. The tasks given to the source and the demands made of him in relation to his activities as a source;
k. All contacts or communications between the source and a person acting on behalf of any relevant investigating authority;
l. The information obtained by each relevant investigating authority by the conduct or use of the source;
m. Any dissemination by that authority of information obtained in that way; and
n. In the case of a source who is not an undercover operative, every payment, benefit or reward and every offer of a payment, benefit or reward that is made or provided by or on behalf of any relevant investigating authority in respect of the source's activities for the benefit of that or any other relevant investigating authority.

The person maintaining these records is the NNDC RIPA Co-ordinator, Kaye Skinner.

Further Documentation

In addition to the above, when appropriate records or copies of the following, as are retained by North Norfolk District Council for 5 years:

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

The records kept by the Council should be maintained in such a way as to preserve the confidentiality, or prevent disclosure of the identity of the CHIS, and the information provided by that CHIS. (Sec 7.7 CHIS Codes of Practice)

The relevant application forms are available in the Appendices which can be found using the attached link:

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

What the Authorising Officer must take into account

1. Must believe that the authorisation is **necessary** for the purposes of preventing and detecting crime or of preventing disorder

2. It is **proportionate** to what it seeks to achieve & appropriate arrangements for managing the source,

3. Should take into account the risk of collateral intrusion,

4. Ensure particular care is taken concerning **confidential material,**

5. Any adverse impact upon the **community confidence,**

6. Assess any **risk to the source.**

7. **Legal advice** obtained from the Council's legal advisors.

Sometimes authorisation is needed in the process of cultivating the source where this would infringe the privacy of the source. The cultivation process itself may require authorisation if it involves directed surveillance, for example.

Authorisations

These work in a similar way to directed surveillance and must be authorised in writing. The use of **vulnerable** sources should only take place in exceptional circumstances. **Juveniles** can never be used as sources against their own parents but can be used subject to special safeguards (see 6.8 below).

Information to be given in applications for authorisation: -

1. Details of the purpose for which the source will be deployed.

2. The grounds on which authorisation is sought (i.e. detection of crime).

3. Where a specific investigation is involved details of that investigation.

4. Details of what the source will be tasked to do.

5. Details of the level of authority required.

6. Details of potential collateral intrusion.

7. Details of any confidential material that might be obtained as a consequence of the authorisation.

Duration of authorisation

A written authorisation (except a juvenile source) is valid for 12 months from the date it took effect.

Reviews and Renewals

An authorisation may be renewed, after the Authorising Officer reviews the use made of the source having regard to:-

a) The tasks given to the source

b) The information obtained from the source.

If satisfied that the original authorisation criteria are met, a renewal may be authorised. A renewal of a grant of a CHIS authorisation must be approved by a Justice of the Peace before it can take place.

Since an authorisation for a CHIS may remain in force for a period of twelve months, regular reviews should be undertaken to ensure the ongoing validity of the activity and the ongoing welfare and security of the source. Any changes to circumstances may require that further risk assessments are undertaken.

The reviews should be undertaken at intervals of **no longer than one month** and documented. Additional **control measures** may also be introduced as a result of a review. The Authorising Officer should implement a system to identify appropriate review dates (e.g. the MS Exchange Calendar alarm option).

Cancellations

An Authorising Officer must cancel an authorisation where:

- The use or conduct of the source no longer meets the original authorisation criteria.

- The procedures for managing the source are no longer in place.
- Where possible the source should be informed of the cancellation, and this fact noted on the cancellation.

Where an investigation no longer requires the authorisation to be in place e.g.the evidence has been obtained, it should be cancelled promptly rather than allowed to expire through time, and the reason for cancellation documented.

Authorisations should be cancelled where the conditions justifying authorisation are no longer satisfied. The Authorising Officer should do this in writing although it is suggested that the officer seeking authorisation should also seek cancellation where s/he becomes aware that the conditions are no longer satisfied. There is a standard form for recording this. Although some authorisations will be renewed on a number of occasions, **every authorisation must be cancelled at the end of the surveillance operation.**

When cancelling an authorisation, an Authorising Officer must ensure that proper arrangements have been made for the activity's discontinuance, including the removal of technical equipment and directions for the management of the product.

Juvenile CHIS

Special safeguards also apply to the use or conduct of juvenile sources; that is sources under the age of 18 years. Authorisation will not normally be granted.

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.

In other cases, authorisations should not be granted unless the special provisions contained within The Regulation of Investigatory Powers (Juveniles) Order 2000 are satisfied.

The use of sources under 16 is dependent on there being an appropriate adult present at any meeting with the Council.

Appropriate adult is defined as:

(a) the parent or guardian of the source;

(b) any other person who has for the time being assumed responsibility for his welfare; or

(c) someone who is otherwise qualified to represent the interests of the source

The Order states that at all times there must be a person within the investigating authority who has responsibility for ensuring that the appropriate adult is present at the meetings.

The duration of such an authorisation is **four months** instead of twelve months.

Restrictions are also imposed on the use of any source under the age of 18. In particular, a person in the investigating authority must make a risk assessment in order to assess the nature and magnitude of any risk of physical injury or psychological distress involved in the proposed course of action, and the person granting the authorisation must be satisfied that the risks are justified and that the source understands the risk and that he has given consideration to the particular relationship, if any, between the source and the target of the authorisation.

7. RECORD KEEPING CHIS

This must be done in such a way as to preserve the confidentiality of the source. The Authorising Officer must not grant an authorisation unless satisfied that there are arrangements in place to ensure that someone has responsibility at all time for maintaining a record of the use made of the source. This should be an officer within the client department and they should record a number of matters (for example, the identity of the source, identities used by the source, how the authority of refers to the source, information about the source's security and welfare, how recruited etc). A full list of the matters to be recorded can be found in paragraph 7.1 to 7.7 of the **CHIS Code**.

Retention and Destruction of Material

The authority must ensure that arrangements are in place for the secure handling, storage and destruction of material obtained through the use or conduct of a CHIS. Authorising Officers must ensure compliance with the appropriate data protection requirements under the UK GDPR and the Data Protection Act 2018.

Where the product of the use or conduct of a CHIS could be relevant to pending or future criminal or civil proceedings, it should be retained in accordance with applicable disclosure requirements under the Criminal Procedures and Investigations Act (CPIA).

There is nothing preventing the material obtained from authorisations for the use or conduct of a CHIS for a particular purpose from being used to further other purposes as long as it does not relate to Legal Privilege material.

JOINT AGENCY SURVEILLANCE

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.

Council staff involved with joint agency surveillance must ensure that all parties taking part are authorised on the authorisation page of the application to carry out the activity. When staff are operating on another organisations authorisation, they should obtain either a copy of the application form (redacted if necessary) or a copy of the authorisation, containing the unique number. This will ensure they see what activity they are authorised to carry out. Their line manager should be made aware of the joint surveillance and a copy of the authorisation forwarded to the central register in order that a record can be retained. This will assist with oversight of the covert activities undertaken by Council staff.

Provisions should also be made regarding any disclosure implications under the Criminal Procedures Act (CPIA) and the management, storage and dissemination of any product obtained.

Surveillance outside of RIPA

As a result of the change in the law from the 1st November 2012, Directed Surveillance under RIPA will only apply to the detection and prevention of a criminal offence that attracts a penalty of 6 months imprisonment or more, or relates to the sale of alcohol or tobacco to children. Therefore, this essentially takes out of RIPA surveillance a lot of offences that the Council may investigate such as disorder (unless it has 6 months custodial sentence) and most summary offences.

Any covert surveillance undertaken without RIPA authorisation loses the Council the benefit of the automatic protection of RIPA which makes all authorised covert activity lawful.

This change does not mean that our enforcement officers cannot undertake such surveillance, but because it is **not now** regulated by the Office of Surveillance Commissioners, they have placed the responsibility to regularly monitor this type of activity on the Councils Senior Responsible Officer (SRO). As a result, we need procedures in place to ensure that we can prove that we have given due consideration to **necessity and proportionality** which are central tenets of European Law and the likely grounds of any challenge that we may receive.

If it is necessary for the Council to undertake surveillance which does not meet the criteria to use the RIPA legislation, such as in cases of disciplinary investigations against staff or surveillance relating to Anti-Social Behavior appertaining to disorder, the Council must still meet its obligations under the Human Rights Act and be able to demonstrate that it's actions to breach someone's article 8 rights to privacy are **necessary and proportionate**, which includes taking account of the intrusion issues. To demonstrate this accountability, the decision making process and the management of such surveillance must be documented. Therefore, should staff have a requirement to undertake covert surveillance which would meet the test of Directed Surveillance, (save for the fact that it does not meet the legal criteria relating to a criminal offence which has a sentence of 6 months imprisonment, or relates to the sale of alcohol and tobacco to children), they should complete the Non RIPA Surveillance form and submit it to one of the RIPA Authorising Officers listed within this policy. The authorisation should be considered by the Authorising Officer before any activity can be undertaken. **There will be no requirement to have the authorisation approved by a Justice of the Peace.** Should the activity be approved, the procedures to be followed will be the same as any RIPA authorised activity. Therefore the Council expects that the procedure and management from the initial surveillance assessment, through to completion and cancellation are to be managed appropriately at the same level that the RIPA legislation and guidance requires.

Internet Investigations and Social Media Enquiries

The internet is a useful investigative tool and social networking sites are easily accessible giving access to a large amount of information which could not otherwise be obtained. However, carrying out these activities is likely to infringe a person's article 8 rights to privacy. The activity may also meet the criteria for Directed Surveillance under RIPA and should be authorised. One of the amendments to the Surveillance Codes of Practice was to take account of this type of activity. The paragraph below is from the Codes:

The use of the internet may be required to gather information prior to and/or during an operation, which may amount to directed surveillance. 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, including the effect of any collateral intrusion. Any activity likely to interfere with an individual's Article 8 rights should only be used when necessary and 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.

The IPCO have stated (quoting from the 2011-12 annual report) that the internet is a surveillance device as per s.48(1) of RIPA and that viewing material on the internet may constitute covert surveillance as just because something is put into the public domain by someone does not mean that they expect it to be read by a public authority as "knowing that something is capable of happening is not the same as an awareness that it is or may be taking place."

The frequent or systematic check on an open source record could amount to directed surveillance and as can be seen from the above, the same considerations of privacy, and especially collateral intrusion against innocent parties, must be applied regardless of the fact that the activity is conducted on line.

An authorisation for the use and conduct of a CHIS is necessary if a relationship is established or maintained by the officer (i.e. the activity is more than mere reading of the site's content). This could occur if an officer covertly asks to become a "friend" of someone on a social networking site. The officer seeking the authorisation should fully consider the issue of collateral intrusion.

A CHIS authorisation is unlikely to be required when using an internet trading organisation such as E-bay or Amazon Marketplace. The use of a disguised purchaser details in a simple, overt, electronic purchase does not usually require a CHIS authorisation, because no relationship is usually established at this stage. A CHIS authorisation is required in circumstances when a covert

relationship is likely to be formed, for example when liaising via Facebook or other types of site which do not allow for more traditional transactions and where the investigating officer has to make contact with the seller directly and would wish for their true identity or reason for purchasing to be unknown to the seller.

When conducting online enquiries when they meet the Directed Surveillance criteria a RIPA authorisation should be sought.

Where the activity does not meet the Directed Surveillance criteria it is essential that detailed notes be made by any officer viewing material on the internet explaining what they were seeking, why it was necessary and proportionate to do so and why prior authorisation was not sought.

Anti-Social Behaviour Activities (e.g. Noise, Violence, Race etc.)

As from 1 November 2012 there is no provision for a Local Authority to use RIPA to conduct covert activities for disorder such as anti-social behaviour, unless there are criminal offences involved which attract a maximum custodial sentence of six months. Should it be necessary to conduct covert surveillance for disorder which does not meet the serious crime criteria of a custodial sentence of a maximum of six months, this surveillance would be classed as surveillance outside of RIPA, and would still have to meet the Human Rights Act provisions of Necessity and Proportionality.

Errors

There is now a statutory requirement under section 231 of the Investigatory Powers Act 2016 to report all covert activity that was not properly authorised to the IPCO in writing as soon as the error is recognised. This would be known as an error. This includes activity which should have been authorised but wasn't or which was conducted beyond the directions provided by the Authorising Officer. It is therefore important that when an error has been identified it is brought to the attention of the SRO in order to comply with this guidance. The Council has a responsibility to report to the Inspector at the commencement of an inspection all activity which should have been authorised but wasn't. This is to confirm that any direction provided by the Investigatory Powers Commissioner has been

followed. This will also assist with the oversight provisions of the Councils' RIPA activity.

This does not apply to covert activity which is deliberately not authorised because an Authorising Officer considers that it does not meet the legislative criteria, but allows it to continue. This would be surveillance outside of RIPA. (See oversight section below)

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

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

- Relevant error and
- Serious error

Relevant Error

An error must be reported if it is a "**relevant error**". A relevant error is any error by a Public Authority in complying with any requirements that are imposed on it by any enactment which are subject to review by a Judicial Commissioner. This would include compliance by public authorities with Part II of the 2000 Act (RIPA). This would include compliance with the content of the Codes of Practice.

Examples of relevant errors occurring would include circumstances where:

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

All relevant errors made by Public Authorities must be reported to the Investigatory Powers Commissioner by the Council as soon as reasonably practicable and a full report no later than ten working days. The report should include information on the cause of the error; the amount of surveillance

conducted, and material obtained or disclosed; any unintended collateral intrusion; any analysis or action taken; whether any material has been retained or destroyed; and a summary of the steps taken to prevent recurrence.

Serious Errors

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

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

Officers must refer to the Codes of Practice for due regard.

COMPLAINTS

The Act establishes an independent Tribunal. This Tribunal will be made up of senior *member*s of the judiciary and the legal profession and is independent of the Government. The Tribunal has full powers to investigate and decide any case within its jurisdiction. This code does not cover the exercise of the Tribunal's functions. Details of the relevant complaints procedure can be obtained from the following address:

Investigatory Powers Tribunal
PO Box 33220
London
SW1H 9ZQ

020 7035 3711