OADBY & WIGSTON BOROUGH COUNCIL

REGULATION OF INVESTIGATORY POWERS ACT 2000 POLICY

March 2015

Committee approval	Policy, Finance and Development Committee – 24 March 2015
Author	Kalv Garcha, Head of Corporate Resources
EIA	26 January 2015
Policy Version Number	2.0
Date of Policy Review	March 2016

Contents

1.	PART 1: Background	3
2.	PART 2: Scope	3
3.	PART 3: Purpose	3
4.	PART 4: General Information on RIPA	4
5.	PART 5: Types of Surveillance	5
6.	PART 6: Covert Human Intelligence Sources ("CHIS")	7
7.	PART 7: Authorisations, Renewals and Cancellations	8
8.	PART 8: Working with Third Parties/Agencies	11
9.	PART 9: CCTV	12
10.	PART 10: Online Covert Activity	12
11.	PART 11: Record Management	12
12.	PART 12: Scrutiny of Authorisations – The Chief Surveillance Commissioner and the Tribunal	14
13.	PART 13:Acquisition and Disclosure of Communications Data	15
14.	PART 14: Training and Guidance	16
15	PART 15: Data Protection	17
16.	PART 16: Review and Monitoring	17

Appendix 1: Examples of Different Types of Surveillance
Appendix 2: Examples of when a CHIS may arise

PART 1: Background

Oadby and Wigston Borough Council ("the Council") has a statutory duty to conduct its covert surveillance activities in accordance with the Regulation of Investigatory Powers Act 2000 ("RIPA" or "the Act"). The use of surveillance (both overt and covert) to provide information is a valuable resource, not only for the protection of the public, but also to maintain law and order. It is essential that such investigations are carried out effectively, efficiently and in accordance with human rights legislation. Consideration must be given, prior to authorisation as to whether or not the surveillance and associated collateral intrusion is necessary and proportionate; whether a potential breach of human rights legislation is justified in the interests of the community as a whole, or whether the information could be obtained in other ways.

There is a requirement for certain investigations to be authorised by an appropriate Officer together with judicial approval. The Office of Surveillance Commissioners (OSC) has been set up as an independent inspection regime to monitor these activities. This policy should be read in conjunction with RIPA, and the Home Office Codes of Practice on Covert Human Intelligence Sources and Covert Surveillance and Property Interference. Please see the link to the Codes of Practice in Part 14.

PART 2: Scope

This policy applies to any employee of the Council who acts as an Investigating Officer or who acts as and Authorising Officer. It will guide Officers from the start of the investigation to the point at which the legal process will begin (which is beyond the scope of this policy).

Officers should act within the scope of their delegated authority and act with due regard to all relevant legislation; including but not limited to RIPA, the Protection of Freedoms Act 2012, Human Rights Act 1998 and the Police and Criminal Evidence Act 1984.

Officers must consider any appropriate codes of practice made under such legislation, and will be guided in their work by the regulations laid down in legislation and underpinning this policy.

PART 3: Purpose

This policy explains how the Council will comply with its legal requirements in relation to the use of surveillance. It seeks to encourage and promote a professional approach ensuring appropriate controls are in place when undertaking surveillance. This will ensure that so that those affected will have confidence that the Council will act effectively.

This policy explains both the circumstances and procedures to be followed in relation to RIPA.

PART 4: General Information on RIPA

The Human Rights Act 1998 requires the Council, and other organisations, pursuant to Article 8 of the European Convention on Human Rights (ECHR), to respect the private and family life of citizens, their home and their correspondence. Notwithstanding this, the ECHR made this a qualified right and so the Council may interfere in the citizen's right, if such interference is:

- In accordance with the law (for issues concerning national security, public safety, economic wellbeing of the country etc);
- Necessary for the prevention and detection of crime or preventing disorder; and
- Proportionate (as defined below)

Proportionality involves balancing the intrusiveness of the activity on the target subject and others who might be affected by it against the need for the activity in operational terms. The activity will not be proportionate if it is excessive in the circumstances. Each case will be judged and be unique on its merits; if the information which is sought could be reasonably obtained by other less intrusive means then these means should be adopted as it would be considered to be more "proportionate". All such activity must be carefully managed to meet the objective in question and must not be arbitrary or unfair. Due diligence should be exercised over any publication of the product of an investigation that concerned surveillance.

RIPA provides a statutory mechanism for authorising covert surveillance and the use of "covert human intelligence sources" ('CHIS'). In certain circumstances, RIPA also permits local authorities to compel telecommunications and postal companies to obtain and release communications data to them. The Act seeks to ensure that any interference with an individual's right under Article 8 of the ECHR is necessary and proportionate. In doing so, both the public interest and the human rights of individuals are suitably balanced.

If the correct procedures are not followed, evidence may be disallowed by the courts, a complaint of maladministration could be made to the Local Government Ombudsman ('LGO'), and/or the Council could be ordered to pay compensation. Such action could tarnish the Council's good reputation and be subject to adverse press and media interest. Therefore, it is essential that all involved with covert investigations comply with this policy and any further guidance or recommendations that may be issued by the Home Office.

The Council treats the powers given to it under RIPA very seriously and expects Investigating Officers and Authorising Officers alike, to do also. Failure to adhere to this policy by either Investigating Officers or Authorising Officers may result in disciplinary action being taken against them by the Council in line with the Disciplinary Policy and Procedure

PART 5: Types of Surveillance

RIPA provides for the authorisation of surveillance by public authorities, where the surveillance is likely to result in the obtaining of private information about a person. It does so by establishing a procedure for authorisation, prescribing the office, rank and position of those permitted to authorise covert surveillance. The authorisation process is subject to judicial approval and so authorisations granted by the Council will **not** take effect unless approved by the Magistrates Court.

What is Surveillance

Surveillance is an essential mechanism in modern life; it not only assists in targeting criminals, but also is a means of protecting the public from harm and preventing crime. In terms of RIPA (section 48(2)), Surveillance includes:

- Monitoring, observing or listening to persons, their movements, their conversations or any of their activities or communications;
- Recording anything monitored, observed or listened to in the course of surveillance; or
- Surveillance by or with the assistance of any surveillance device.

Surveillance can be overt or covert.

Overt Surveillance

Most of the surveillance carried out by the Council will be done overtly; there will be nothing secretive, clandestine or hidden about it. In many cases, Officers will be behaving in the same way as a normal member of the public (e.g. in the case of most test purchases), and/or will be going about Council business openly (e.g. parking wardens walking through town centres). This list is not exhaustive.

Similarly, surveillance will be overt if the subject has been told it will happen. Examples include, where a noisemaker is warned (preferably in writing) that noise will be recorded if it continues, or where an entertainment licence is issued subject to conditions, and the licensee is told that Officers may visit without notice or identifying themselves to the owner/ proprietor to check that the conditions are being met.

Covert Surveillance

Surveillance is covert if it is carried out in a manner calculated to ensure that the person subject to the surveillance is unaware that it is or may be taking place (Section 26(9)(a) of RIPA). It cannot, however, be deemed necessary and proportionate if there is reasonably available overt means of finding out the information desired.

RIPA governs three types of covert surveillance: Intrusive Surveillance, Directed Surveillance and the use of Covert Human Intelligence Sources (CHIS).

Intrusive Surveillance

This is when surveillance is:

- Covert
- Relates to residential premises and/or private vehicles; and

- Involves the presence of a person in the premises or in the vehicle or is carried out by a surveillance device in the premises/vehicle. 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.

Examples include, surveillance of a place ordinarily used for legal consultation; at a time when they are being used for such consultations is also a form of intrusive surveillance.

However, areas of a building that are really visible and accessible to the public are not residential premises; for example a canteen, reception area or a garden. This list is not exhaustive.

Intrusive surveillance can only be carried out with the approval of the Surveillance Commissioners as it should only relate to an investigation in relation to serious crime and thus is dealt with by the police**. Intrusive surveillance cannot be conducted or approved by the Council as it has no statutory powers to interfere with private property.**

Directed Surveillance
This is when surveillance is:

- Covert,
- Not intrusive surveillance (see definition below),
- Not carried out in an immediate response to events which would otherwise make seeking authorisation under the Act unreasonable e.g. spotting something suspicious and continuing to observe it,
- Pre-planned,
- Undertaken for the purpose of a specific investigation or operation in a manner likely to obtain private information about an individual whether or not that person is specifically targeted for purposes of an investigation (Section 26 (10) of RIPA).

Directed Surveillance can only be authorised for investigating serious criminal offences. “Serious” means criminal offences that are punishable, whether on summary conviction or on indictment, by a maximum term of at least 6 months of imprisonment. Serious criminal offences would include dangerous waste dumping and serious or serial benefit fraud. Thus the Council cannot carry out directed surveillance for offences that would only result in a fine or less than 6 months imprisonment, such as littering or dog fouling.

It is crucial that Investigating Officers consider the penalty attached to the criminal offence which they are investigating before considering whether authorisation for directed surveillance should be obtained**.**

Private information in relation to a person includes any information relating to their private family life, their home, their correspondence, and their business relationships. The mere fact that covert surveillance occurs in a public place or on business premises does not mean that it cannot result in the obtaining of private information about a person. Prolonged surveillance targeted on a single person will undoubtedly result in attaining private information about them and others that they come in contact, or associate with.

Similarly, although overt town centre CCTV cameras do not ordinarily require authorisation, if the camera(s) are to be directed for a specific purpose to observe particular individual(s), authorisation **will** be required. The way a person runs their business may also reveal information about their private life and the private lives of others.

For the avoidance of doubt, Authorising Officers can authorise "Directed Surveillance" for the purposes of RIPA **only** if the RIPA authorisation procedures detailed in this policy below are followed.

Please see **Appendix 1** for a non exhaustive list of examples of the different types of surveillance.

PART 6: Covert Human Intelligence Source ("CHIS")

The Council may grant an authorisation under RIPA for the use of a Covert Human Intelligence Source ("CHIS"). The conduct that may be authorised is any conduct that:

- Is comprised in any such activity including the conduct of CHIS or use of CHIS, as are specified in the authorisation;
- Consists in conduct by or in relation to a person who is so specified or described as a person as to whose actions as a CHIS the authorisation relates;
- Is carried out for the purposes of or in connection with the investigation or operation so specified or described; and
- Is necessary and proportionate to the intelligence that it seeks to achieve.

A person is considered to be a CHIS (also known as a relevant source) if he or she establishes or maintains a personal or other relationship with a person for the covert purpose of either:

- Obtaining information or provide access to any information to another person; or
- Disclosing information obtained by the use of the said relationship, or as a consequence of the existence of such a relationship.

The application form is the same as for directed surveillance. In addition the authorisation must specify the activities and identity of the relevant source and that the authorised conduct is carried out for the purposes of, or in connection with, the investigation or operation so specified. All application forms must be completed with the required details to enable the Authorising Officer to make an informed decision.

Authorisations do not relate solely to the obtaining of private information. An authorisation is necessary where there is covert manipulation of a relationship to gain any information. Article 8 of the ECHR includes the right to establish and develop a relationship, so such a right may be infringed where a local authority manipulates that relationship to obtain information.

To establish a relationship simply means to "set up" a relationship and does not require endurance of a relationship over a period of time. The use of a relevant source is most likely to arise when individuals develop a relationship with a person;

for example in a shop to obtain information about the seller's suppliers of an illegal product. Therefore, simply making the test purchase does not require such authorisation nor does a repetition of purchases.

The Home Office has strongly recommended that local authorities should consider an authorisation whenever the use or conduct of a relevant source is likely to engage an individual' rights under Article 8 of the ECHR. The Council must acknowledge that a CHIS may appear at any time and so the Council must conduct a risk assessment to manage them by assessing whether conduct is likely to engage rights under Article 8 of the ECHR.

Before authorising the use of CHIS a risk assessment must be carried out and a system must be implemented to manage the relevant source (usually done by an an Officer who will be referred to as the manager of the relevant source). There must also be a person appointed to take responsibility for the day to day activities of the source, this will include the recording of the information gained. This person will be called the handler of the source.

Please note, not all activity will satisfy the definition of a CHIS. For example, a source may be a public volunteer who discloses information out of professional or statutory duty. Further, individuals may merely volunteer to provide information that is within their personal knowledge, without being asked by the public authority. Where such a situation would arise, the individual who provided the information (referred to as a "public volunteer") would not be amount to a CHIS for the purposes of RIPA; thus no authorisation under RIPA is required.

To see examples of when a CHIS would arise please see **Appendix 2.**

PART 7: Authorisations, Renewals and Cancellations

It is essential the relevant forms of covert surveillance are authorised in accordance with the provisions of RIPA. Regulations prescribe that, within the Council, the Authorising Officer must hold the rank of Chief Executive, Director, Head of Service or equivalent.

List of Authorising Officers

Mark Hall	Chief Executive (also RIPA Authorising Officer)
Anne Court	Director of Services (also RIPA Senior Responsible Officer)
Kalv Garcha	Head of Corporate Resources (also RIPA Monitoring Officer)

All authorisations under RIPA are for specific investigations only. These must be reviewed, renewed or cancelled once the specific surveillance is complete or about to expire. The authorisations do not lapse with time.

Application Forms

Authorisations must be obtained using the Home Office approved forms. Any other forms used will be rejected by the Authorising Officer and/or the Head of Corporate Resources. All the relevant RIPA forms can be found on the Home Office website: https://www.gov.uk/government/collections/ripa-forms--2. If an Officer is unsure of which form to use, they should consult with a member of the Legal Team.

Assessing the Application Form
Before an Authorising Officer signs an application form, they must:

- Be mindful of this policy, the training provided and any other guidance issued, from time to time by the Home Office on such matters.

- Satisfy themselves that the RIPA authorisation is:-

    - In accordance with the law;
    - Necessary in the circumstances of the particular case and on the grounds of preventing or detecting crime or preventing disorder;
    - For directed surveillance, it must be necessary for the investigation of a serious criminal offence; and
    - Proportionate to what it seeks to achieve (see above in Part 4)

- The Authorising Officer must take a number of things into consideration when assessing the proportionality of covert surveillance. He must:

    - Balance the size and scope of the proposed activity against the gravity and extent of the perceived crime or offence;
    - Explain how and why the methods to be adopted will cause the least possible intrusion on the subject and others;
    - Consider whether the activity is an appropriate and reasonable use of the legislation by taking into consideration all reasonable alternatives of obtaining the necessary result including overt methods of evidence gathering;
    - Evidence, as far as reasonably practicable what methods had been considered and why they were not implemented;
    - Take into account the risk of intrusion into the privacy of persons other than the specified subject of the surveillance (this is collateral intrusion). Measures must be taken, wherever practicable, to avoid or minimise (so far as is reasonable) collateral intrusion and the matter may be an aspect of determining proportionality;
    - Set a date for review of the authorisation and review on that date using the relevant form. Authorisations for directed surveillance should be reviewed at least once a month;
    - Ensure that a copy of all RIPA forms (applications, reviews, renewals and cancellations) are forwarded to the Head of Corporate Resources as soon as possible;
    - If unsure on any matter, obtain advice from the Legal Team before signing any forms.

Please note, the least intrusive method will be considered proportionate by the courts.

Urgent Authorisations
For urgent grants or renewals, oral authorisations are acceptable but should be followed up with a written application within 24 hours of the verbal authorisation being given. Urgent grants are those where authorisation would be needed but the circumstances are such that if a granted was waited for then the time for gathering of the information would have passed and the opportunity missed. Urgent oral authorisations will, unless renewed, cease to have effect after 72 hours, beginning

with the time when the authorisation was granted. The December 2014 issue of the Home Office guidance states that local authorities are no longer able to orally authorise the use of RIPA techniques and so the out of hours service needs to be used or the application would need to wait until the next day.

Magistrates Approval

After the Authorising Officer has signed the RIPA application form, it must be approved by a Magistrate before the operation can commence. The Investigating Officer should liaise with the Legal Team to seek this authorisation. The relevant individual within the Legal Team will arrange a hearing with the court to seek the Magistrate's approval. They should provide the court with the correctly executed RIPA application form and supporting information. The Investigating Officer and the Authorising Officer will be required to attend court with the Council's Solicitor to seek the Magistrates Approval.

Guidance on the procedure for seeking Magistrates approval can be found at: https://www.gov.uk/government/publications/changes-to-local-authority-use-of-ripa

Duration

An authorisation must be reviewed or renewed in the time stated or cancelled once it is no longer needed. Authorisation to carry out directed surveillance lasts for a maximum of 3 months from authorisation. The authorisation does not expire and has to be reviewed, renewed and/or cancelled once it is no longer required.

With regards to a CHIS, a written authorisation will, unless renewed, cease to have effect at the end of a period of 12 months beginning with the day on which it took effect, except in the case of juvenile CHIS. The authorisation for a juvenile (those under 18 years old) as a CHIS can only be for one month from the time of grant or renewal. For the purpose of these rules, the age test is applied at the time of the grant or renewal of the authorisation.

The approval from the Magistrates Court is required to renew an authorisation. Authorisations must be renewed in writing before the maximum period in the authorisation has expired. The Authorising Officer must consider the matter afresh, taking into account the benefits of the surveillance to date, and any collateral intrusion that has occurred. Magistrates' approval will then be required. An authorisation cannot be renewed after it has expired. Should such an event occur, a fresh application will be necessary.

Reviews and Renewals

Regular reviews should be carried out throughout the duration of the authorisation to assess the need for the surveillance to continue. Authorising Officers should determine how often a review should take place. This should be as frequently as considered necessary and practicable, but at no longer than monthly intervals. If at any time before the time and day on which the authorisation expires the Authorising Officer, or, in their absence the designated deputy considers the authorisation should continue to have effect for the purpose for which it was issued, he or she may renew it in writing for a period of 3 months beginning with the day on which the authorisation would otherwise have cease to have effect. There is no requirement for the Magistrates Court to consider any internal review for an authorisation. With regards to a CHIS, the authorisation may be renewed for a further period of one month after a thorough review has been carried out and the Authorising Officer has

considered the results. A review must cover what use has been made of the source, the tasks given to them and the information obtained.

Cancellations

During a review, the Authorising Officer who granted or last renewed the authorisation may amend specific aspects of it. As soon as the decision is taken that directed surveillance should be discontinued, the instruction must be given to those involved to stop all surveillance of the subject(s). The date the authorisation was cancelled should be centrally recorded and documentation of any instruction to cease surveillance should be retained. There is no requirement for any further details to be recorded when cancelling a directed surveillance authorisation. Effective practice suggests that a record should be retained detailing the product obtained from the surveillance and whether or not objectives were achieved. There is no requirement for the Magistrates Court to consider cancellations of authorisations.

For further information on record management and the Central Register, please see Part 11 below.

Refusal of approval of long-term authorisation – CHIS Only

If an Ordinary Surveillance Commissioner does not conclude a long term authorisation, the Council can appeal against the decision to the Chief Surveillance Commissioner within 7 days. Any risk assessment produced for a CHIS should include details of how they can be safely extracted should authorisation from a Surveillance Commissioner be refused.

PART 8: Working with Third Parties/Agencies

When an agency or third party has been instructed to work on the Council's behalf to undertake any action under RIPA, both this policy and the Home Office approved application forms must be used (as per the procedure outlined above) and the agency advised or kept informed, as necessary, of the various requirements. It is essential that authorisation is obtained and that the relevant agency is explicitly aware of what they are authorised to do.

When another agency (e.g. Police, DWP, Trading Standards etc) wishes to use the Council's resources (e.g. CCTV surveillance systems), that agency must use its own RIPA procedures. Prior to any Officer agreeing to allow the Council's resources to be used, they must obtain a copy of that agency's RIPA form for the Council's Central Register. This is to protect the Council and the use of its resources. If another agency wishes to use the Council's resources for their own RIPA actions, and is expressly seeking assistance from the Council, the Officer should, co-operate with the same, unless there are security or other good operational or managerial reasons as to why the Council's premises should not be used for the agency's activities. Suitable insurance or indemnities may be sought, if necessary, from the other agency, at their expense, for the Council's cooperation in the agent's RIPA operation. In such cases, the Council does not require its own RIPA form as the Council is merely "assisting" as opposed to being "involved" in the RIPA activity of the external agency.

If the Police or another agency wishes to use Council resources for general surveillance, as opposed to specific RIPA operations, an appropriate letter requesting the proposed use, extent of remit, duration, who will be undertaking the surveillance and the purpose of it must be obtained from the Police or agency before any Council resources are made available for the proposed use. Please ensure that the Legal Team are consulted before anything is embarked upon.

PART 9: CCTV

The use of overt CCTV cameras by local authorities does not normally require an authorisation under RIPA. Members of the public should be made aware that such systems are in use; for example, by virtue of cameras or signage being clearly visible. Please refer to the Council's CCTV Policy for further information.

Before an application for surveillance using a camera is made the matter must be considered by the Council's CCTV Group to assess feasibility. An Officer must then complete an application form with the required details for authorisation by the Authorising Officer. No authorisation shall be granted unless the Authorising Officer is satisfied that it is both necessary and proportionate (as mentioned in Part 4 above). Advice should be sought from the Legal Team on any issues of concern.

Once authorisation has been granted, steps must be taken to avoid, if not minimise collateral intrusion. Investigating Officers must inform the Authorising Officer of any unexpected interference with the privacy of individuals who are not covered by the authorisation (collateral intrusion), as soon as they become apparent.

PART 10: Online Covert Activity

The use of the internet may be required to gather information during an operation, which may amount to directed surveillance. The Home Office advises that where there is an intention to use the internet as part of an investigation and private information is likely to be obtained, consideration should be given for the need of an authorisation. Further, where an investigator may need to communicate covertly online, for example, contacting individuals using social media websites, a CHIS authorisation should be considered.

PART 11: Record Management

It is essential that the Council keep a detailed record of all authorisations, reviews, renewals, cancellations and rejections for each respective service area. A Central Register ("the register") of all authorisation forms will be maintained and monitored by the Head of Corporate Resources (RIPA Monitoring Officer) via the Compliance Officer. All original forms must be sent to the Head of Corporate Resources as soon as practicable; ideally within 1 week of the relevant authorisation, review, renewal, cancellation or rejection.

All of the information relating to the authorisation will form part of the records of the investigation. A record will be retained detailing the product obtained from the surveillance and whether or not objectives were achieved. Information that may be of value in connection with concurrent investigations may be kept, but information not relevant to those enquiries must be destroyed.

In line with the Home Office guidance, the register must be retrievable for at least 3 years from the ending of each authorisation. Good practice suggests such records should be kept for 5 years in the event of an appeal being made. All documents must be treated as strictly confidential, and Authorising Officers must make appropriate arrangements for their retention, security and destruction following the Council's Data Protection Policy and the RIPA Codes of Practice.

The Investigating Officer should keep the following records and diarise the dates for review, renewal and cancellation:

- The type of authorisation;
- The date the authorisation was given;
- Name and position of the Authorising Officer;
- The Unique Reference Number (URN) of the investigation;
- The title of the investigation, including a brief description and names of the subjects if known;
- A copy of the authorisation together with supporting documents;
- A copy of any renewal of any authorisation together with supporting documents, the date of renewal and the name and position of the Authorising Officer;
- Any authorisation which was granted or renewed urgently and the reason why the authorisation was considered to be urgent ;
- Whether any confidential information is likely to be obtained from the investigation or operation;
- Any risk assessment raised in relation to a CHIS;
- The circumstances in which tasks were given to the CHIS;
- The value of the CHIS to the investigation;
- A record of the results of any reviews of the authorisation;
- The reasons for not renewing an authorisation;
- The reasons and date for cancelling an authorisation; and
- The date and time when any instructions were given by the Authorising Officer since using a CHIS.

In using CHIS, the records should be maintained so as to preserve the confidentiality of the source and the information provided by the source.

The documentation mentioned below, should also be centrally retrievable for at least 3 years from the ending of each authorisation:

- A copy of the application and a copy of the authorisation together with any supplementary documentation and notification of the approval given by the Authorising Officer;
- A record of the period over which the surveillance has taken place;
- The frequency of reviews prescribed by the Authorising Officer
- A record of the result of each review of authorisation
- A copy of any renewal of authorisation, together with the supporting documentation submitted when the renewal was requested;
- 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 copy of the order approving or otherwise the grant or renewal of an authorisation from a Magistrate (Justice of the Peace).
- (For CHIS only) A copy of the decision by an Ordinary Commissioner on the renewal of an authorisation beyond 12 months.

PART 12: Scrutiny of Authorisations – The Chief Surveillance Commissioner and the Tribunal

The Chief Surveillance Commissioner and Inspections

The Chief Surveillance Commissioner reviews the exercise and performance of the use of authorisations by public bodies. Information must be provided on request and inspections are carried out regularly by the Chief Surveillance Commissioner's staff ("the Inspector").

The Council must bring the following situations to the attention of the Inspector at the next inspection:

- Where an Officer has had to authorise surveillance in connection with an investigation in which he is directly involved;
- Where a lawyer is the subject of an investigation or operation;
- Where confidential personal or confidential journalistic information has been acquired and retained.

The Tribunal

This has been established to consider and determine complaints relating to the exercise of RIPA powers by any aggrieved person. The tribunal deals with these matters in a similar manner to the courts when dealing with judicial review cases. Complaints must be lodged with the tribunal within one year unless the tribunal determines it is just and equitable to extend that period. The tribunal may order the quashing or cancellation of any authorisation, records or information obtained by use of an authorisation.

The Council is under a duty to disclose to the tribunal all documents that may be required relating to the authorisation if:

- A Council Officer has granted any RIPA authorisations;

- Council employees have engaged in any activity as a result of such authorisation; or if
- A disclosure notice is given.

PART 13: Acquisition and Disclosure of Communications Data

Part 1 Chapter 2 sections 21-25 of RIPA 2000, regulates the acquisition and disclosure of communications data. It provides powers for the Council to gain communications information when carrying out investigations. The Code of Practice on the Acquisition and Disclosure of Communications Data should be followed (and the link is available in Part 14 below).

Definition of communications data (S21) (4) RIPA)

Local Authorities are only permitted to gain access to two types of communications data:-

- **Service Data**: This is information held by a telecom or postal service on the use made of a service by any person, for example itemised telephone records;
- **Subscriber Data**: This is any other information or account details that a telecom or postal service provider holds on a person under investigation;

Local Authorities are not authorised to obtain Traffic Data. This is information about when communications were made, who from and who to. Further, these powers do not permit access to the contents of the communication.

Purpose for the use of Communications data

Local Authorities may only gather communications data for the purpose of the prevention and detection of crime or preventing disorder; for example a benefit fraud investigator may be able to get access to an alleged fraudster's mobile phone bills.

Procedure for the authorisation of the acquisition and disclosure of communications data

The process is similar to that of the authorisation of directed surveillance and CHIS but has extra provisions and procedures. All requests to obtain communications data must be in writing on the application form from the Council's intranet site. Authorisation must be by an Authorised Officer.

Authorisation must only be granted where access to communications is believed to be necessary and proportionate by the Authorising Officer. Communications data will be obtained either via authorisation for the authority to collect the data itself under Section 22(3) RIPA or by a notice under Section 22(4) to a postal or telecommunications operator to collect or retrieve the date and provide it to the local authority.

Single Point of Contact (SPOC)

Notices and authorisations for communications data should be channelled through a SPOC. The role of the SPOC is to:-

- Assess whether it is reasonably practicable to obtain the communications data requested;
- To advise applicants/Authorising Officers on the types of communications data that can be obtained
- To check that the application form is properly completed and authorised; and
- To liaise with the service providers on obtaining the communications data requested

All SPOC's must attend an accredited course and obtain a PIN reference from the Home Office before they may act as a SPOC. The PIN reference number is given to the service provider with each request for data, so that the service provider can be sure that they are providing the data to a properly accredited and authorised person within the Authority. The Director of Services is the SPOC for Oadby and Wigston Borough Council.

Oral Authority
Oral authority is not permissible by local authorities.

Duration
Authorisations and Notices are only valid for one month from the date when it was granted. If the information can be collected in a shorter period, that should be specified to accord with the proportionality element of the decision making.

Renewal
An authorisation or notice can be renewed within that month if a fresh application or authorisation is made following the same procedure as in obtaining a fresh authorisation.

Cancellations
It is the duty of the Authorising Officer to cancel the authorisation as soon as it is no longer necessary or proportionate to what is being sought to be achieved. The Authorising Officer must inform the SPOC in writing, who will then cancel the Notice served on the service provider. Authorising Officers must record the cancellation on the original application form retained by the SPOC.

Retention
Applications, authorisations and Notices will be retained by the Authority until they have been audited by the Commissioner. The originals should be kept in the Central Register.

PART 14: Training and Guidance

Training on this Policy shall be given to the relevant Council Officers who may be required to carry out investigations as and when applicable, by a representative of Corporate Resources (under the instruction of the Head of Corporate Resources).

In complying with RIPA, local authorities must have full regard to the Codes of Practice issued and revised by the Home Office, pursuant to S71 of RIPA. The links to the relevant codes are downloadable by following the link below:

https://www.gov.uk/government/collections/ripa-codes

The Office of Surveillance Commissioners has produced a Procedures and Guidance publication: this shall be made available to relevant staff, and their attention shall be drawn to the passages referring to the use of social networking websites for investigative purposes.

PART 15: Data Protection

Information obtained under RIPA's powers is likely to be "personal data" within the meaning of the Data Protection Act 1998. The requirements of the Data Protection Act and its principles must be adhered to in respect of this data. For further guidance on the Data Protection Act please see:
https://ico.org.uk/media/fororganisations/documents/1607/the_guide_to_data_protection.pdf

PART 16: Review and Monitoring

Elected members of the Council should review the Council's use of the 2000 Act and set the policy at least once a year. They should also consider internal reports on the use of the 2000 Act on a regular basis to ensure that it is being used consistently with the Council's policy and that the policy remains fit for purpose. Elected members will **not** be involved in any decisions made on specific authorisations granted.

The Head of Corporate Resources reserves the right to make amendments to this Policy in the event of changes to legislation, case law or guidance from the Home Office or the Office of Surveillance Commissioners.

Appendix 1 – Examples of different types of Surveillance

Type of Surveillance	Examples
Overt	Police Officer or Park Warden on patrol Signposted town centre CCTV cameras (in normal use) Recording noise coming from outside a premises after the occupier has been warned (preferably in writing) that this will occur if the noise persists) Most test purchases (where the Officer behaves no differently from a normal member of the public)
Covert not requiring prior authorisation	CCTV cameras providing general traffic, crime or public safety information.
Covert RIPA authorisation required	Covert CCTV cameras at a fly-tipping hotspot Covert and targeted following a benefit claimant who is suspected of failing to declare earnings from a job
Intrusive or interfering with private property (NOTE: The Council **CANNOT** do this)	Planting a listening or other electronic device or camera in a person's home, vehicle or on their person. Surveillance of a place used for legal consultations.

Appendix 2 – Examples of when a CHIS may arise.

Example	Information
Test Purchasing	When a child or young person is instructed to carry out a test purchase in a shop, for example, buying alcohol, the Investigating Officer should consider whether that child may be a CHIS and whether it is appropriate to seek a CHIS authorisation. In those circumstances, any relationship between the buyer and seller, if established at all, is likely to be so limited that the Investigating Officer may conclude that a CHIS authorisation is unnecessary. Whether or not a CHIS authorisation is considered to be appropriate, where covert technical equipment is worn by a test purchaser or an adult is observing the test purchase, then an authorisation for directed surveillance may be required. In all cases a prior risk assessment should be undertaken in relation to the test purchaser.
Public Volunteers	Not every human intelligence source will be a CHIS. Example 1: If someone volunteers information to the Council without being induced, asked or tasked by the Council, no authorisation under RIPA is required**.** If a member of the public were to provide a piece of information about something he has witnessed in his neighbourhood, he would not be regarded as a CHIS as the information he is passing is not as a result of a relationship which has been established or maintained for a covert purpose. Example 2: if a member of the public is asked by an Investigating Officer to maintain a record of vehicles arriving at and leaving a specific location, no relationship has been established or maintained in order to gather that information. A CHIS authorisation is therefore not required. There may be a need to obtain a RIPA authorisation for directed surveillance however. In contrast, if an Investigating Officer wishes to use a neighbour to question an individual about the activities carried on at a site which for example, was subject to enforcement action under the Planning Acts, this may amount to the use of a CHIS.
Professional or Statutory Duty	Any regulatory or professional disclosure made by an individual should not result in that individual falling within the definition of a CHIS, as the information disclosed is derived from a business relationship which will not have been established for the covert purpose of disclosing such information. In addition, such disclosure is

Further Guidance on the Use of a CHIS

Further guidance on the use of a CHIS may be found in the Home Office's Code of Practice for the use of human intelligence sources and on the website of the Office of Surveillance Commissioners, the watchdog responsible for overseeing the use of covert surveillance by public authorities based in the UK:

http://surveillancecommissioners.independent.gov.uk/