APPENDIX B

NEWARK & SHERWOOD DISTRICT COUNCIL

Policy on Regulation of Investigatory Powers Act 2000 (RIPA)

Revised: November 2016

NEWARK & SHERWOOD DISTRICT COUNCIL

REGULATION OF INVESTIGATORY POWERS ACT 2000 (RIPA)

POLICY

CONTENTS

SCHEDULE 1

List of the Council's Designated Persons/Authorising Officers, Senior Responsible Officer and RIPA Co-ordinating Officer

NEWARK & SHERWOOD DISTRICT COUNCIL

POLICY ON REGULATION OF INVESTIGATORY POWERS ACT 2000 (RIPA)

COVERT SURVEILLANCE

1.0 Purpose

The purpose of this Policy and accompanying guidance is to explain:

- the scope of RIPA – Chapter 2 of Part 1
- the circumstances where it applies, and
- the authorisations procedures to be followed.

2.0 Introduction

2.1 This policy sets out Newark & Sherwood District Council's ("the Council") position in relation to RIPA. It sets out the practice to be followed before any covert surveillance is undertaken. The Council only carries out covert surveillance where such action is necessary, proportionate and justified and endeavours to keep such surveillance to a minimum. It recognises its obligation to comply with RIPA when such an investigation is for the purpose of preventing or detecting crime or preventing disorder and has produced this document as guidance to assist officers. The procedures and guidance set out in this Policy are based on the provisions of RIPA, the Home Office Codes of Practice on Covert Surveillance and CHIS, the Home Office guidance to Local Authorities in England and Wales on the judicial approval process for RIPA and the crime threshold for directed surveillance and guidance issued by the Office of Surveillance Commissioners. See http://www.homeoffice.gov.uk/counter-terrorism/regulation-investigatory-powers/ripa-codes-of-practice/ and http://www.homeoffice.gov.uk/publications/counter-terrorism/ripa-forms/local-authority-ripa-guidance/ and http://surveillancecommissioners.independent.gov.uk/.

2.2. Officers should be aware of the scope and extent of activities covered by the provisions of RIPA. In many cases, investigations carried out by Council officers will not be subject to RIPA, as they involve overt rather than covert surveillance (see below).

2.3. RIPA **does**:

- require prior authorisation and judicial approval of directed covert surveillance.
- prohibit the Council from carrying out intrusive surveillance.
- require prior authorisation and judicial approval of the conduct and use of a CHIS.
- require safeguards for the conduct and use of a CHIS.

2.4 RIPA **does not**:

- prejudice any existing powers available to the Council to obtain information by any means not involving conduct requiring authorisation under RIPA. For example, it does not affect the Council's current powers to obtain information via the DVLA or from the Land Registry as to the ownership of a property.
- Authorise the use of directed covert surveillance unless the crime threshold is met

3.0 Applications for Authorisations

3.1 The Council's designated Authorising Officers will consider all applications for authorisation in accordance with RIPA. Schedule 1 of this policy identifies each of the officers authorised to act as the Council's designated persons. Any incomplete or inadequate application forms will be returned to the Applicant Officer for amendment. The Authorising Officer shall in particular ensure that:-

- They are investigating a criminal offence;
- There is a satisfactory reason for carrying out the surveillance;
- The crime threshold is met or the offences relate to the underage sale of alcohol or tobacco;
- The covert nature of the investigation is necessary;
- Proper consideration has been given to collateral intrusion;
- The proposed length and extent of the surveillance is proportionate to the information being sought;
- The authorisations are reviewed and cancelled;
- Records of all authorisations are sent to Legal Services for entry on the Central Register;
- An analysis of alternative methods, other than directed covert surveillance has been considered as a way of obtaining the necessary information together with reasons why those alternatives are inappropriate. This is to ensure that RIPA powers are used as a last resort;
- Once authorisation has been obtained from the Authorising Officer the Applicant Officer will attend the Magistrates' Court in order to obtain Judicial approval for the authorisation.

3.2 The Act, which came into force in 2000, regulates the use of investigatory powers exercised by various bodies including Local Authorities, and ensures that they are used in accordance with human rights. This is achieved by requiring certain investigations to be authorised by an appropriate officer and that, judicial approval is obtained before they are carried out.

3.3 The investigatory powers, which are relevant to a Local Authority, are **directed covert surveillance** in respect of specific operations involving criminal offences that are either punishable, whether on summary conviction or indictment by a maximum term of at least six months imprisonment, or are related to the underage sale of alcohol and tobacco and the use of **covert human intelligence sources (CHIS)**. The Act makes it clear for which purposes they may be used, to what extent, and who may authorise their use. There are also Codes of Practice in relation to the use of these powers and these can be viewed at http://www.homeoffice.gov.uk/counter-terrorism/regulation-investigatory-powers/ripa-codes-of-practice/.

3.4 Consideration must be given, prior to authorisation as to whether or not the acquisition of private information is necessary and proportionate, i.e. whether a potential breach of human right is justified in the interests of the community as a whole, or whether the information could be obtained in other ways.

4.0 Scrutiny and Tribunal

4.1 The Council has to obtain an order from a Justice of the Peace approving the grant or renewal of any authorisation for the use of directed surveillance or CHIS before the authorisation can take effect and the activity be carried out. The Council can only challenge a decision of the Justice of the Peace on a point of law by way of judicial review

4.1 The Office of Surveillance Commissioners (OSC) was set up to oversee and monitor compliance with RIPA operations carried out by public authorities. The OSC has *"a duty to keep under review the exercise and performance by the relevant persons of the powers and duties under Part II of RIPA"*, and the Surveillance Commissioner will from time to time inspect and examine the Council's policies, records, operations and procedures for this purpose.

4.2 In order to ensure that investigating authorities are using the powers properly, the Act also establishes a Tribunal to hear complaints from persons aggrieved by conduct, e.g., directed surveillance. Applications will be heard on a judicial review basis. Such claims must be brought no later than one year after the taking place of the conduct to which it relates, unless it is just and equitable to extend this period.

4.3 The Tribunal can order:

- Quashing or cancellation of any warrant or authorisation;
- Destruction of any records or information obtained by using a warrant or authorisation;
- Destruction of records or information held by a public authority in relation to any person.

4.4 The Council has a duty to disclose to the tribunal all documents they require if any Council officer has:

- Granted any authorisation under RIPA;
- Engaged in any conduct as a result of such authorisation.

5.0 Benefits of RIPA Authorisations

5.1 The Act states that if authorisation is given to engage in a certain conduct and the conduct undertaken is in accordance with the authorisation (including judicial approval), then it will be lawful for all purposes. Consequently, RIPA provides a defence to an accusation of an infringement of a human right.

5.2 Material obtained through properly authorised covert surveillance is admissible evidence in criminal proceedings.

6.0 Statutory Definitions

6.1 'Surveillance' includes:-

- monitoring, observing, listening to people, watching or following their movements, listening to their conversations and other such activities or communications.
- recording anything mentioned above in the course of surveillance.
- surveillance by, or with the assistance of, appropriate surveillance device(s).

Surveillance can be overt or covert.

6.2 **Overt surveillance** will include most of the surveillance carried out by the Council - there will be nothing secretive, clandestine or hidden about it. For example, signposted CCTV cameras normally amount to overt surveillance (but see 7.3 below). 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 carried out by Environmental Health for food hygiene or other purposes), and/or will be going about Council business openly (e.g. a parking attendant walking through a Council car park).

6.2.1 Similarly, surveillance will be overt if the subject has been told it will happen. This will be the case where a noisemaker is warned that noise will be recorded if the noise continues; or where an entertainment licence is issued subject to conditions, and the licensee is told that officers may visit without notice or without identifying themselves to the owner/proprietor to check that the conditions are being met. Such warnings should be given to the person concerned in writing.

6.2.2 Overt surveillance does not require any authorisation under RIPA. Neither does **low-level surveillance** consisting of general observations in the course of law enforcement (for example, where a planning officer drives past a site to check whether planning conditions are being complied with). Repeated visits may amount to systematic surveillance, however, and require authorisation: if in doubt, legal advice should be sought. Home Office guidance also suggests that the use of equipment such as binoculars or cameras, to reinforce normal sensory perception by enforcement officers as part of *general* observation does not need to be regulated by RIPA, as long as the *systematic* surveillance of an individual is not involved.

6.3 **Covert surveillance** is surveillance 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. RIPA requires the authorisation of two types of covert surveillance (**directed surveillance** and **intrusive surveillance**) plus the use of CHIS.

6.4 **Directed surveillance** is surveillance which:

- is covert; and
- is not intrusive surveillance (see definition below - the Council is prohibited by law from carrying out any intrusive surveillance);
- is not carried out in an immediate response to events where it would not be practicable to obtain authorisation under the Act;
- is 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).

6.5 **Private information** in relation to a person includes any information relating to his private and family life, his home and his correspondence. The 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. The way a person runs their business may also reveal information about their private life and the private lives of others. Prolonged surveillance targeted on a single person will undoubtedly result in the obtaining of private information about them and others that s/he comes into contact or associates with.

6.6 Similarly, although signposted town centre CCTV cameras do not normally require authorisation, this will be required if the camera is tasked for a specific purpose which involves prolonged surveillance on a particular person or place.

6.7 Other examples of directed surveillance include:

- officers following an individual over a period to establish whether they are working whilst claiming benefit
- test purchases where a hidden camera or other recording device is used.

6.8 Surveillance that is unforeseen and undertaken as **an immediate response** to a situation normally falls outside the definition of directed surveillance and, therefore, authorisation is not required. However, if a specific investigation or operation is subsequently to follow, authorisation must be obtained in the usual way before it can commence. In no circumstance will any covert surveillance operation be given backdated authorisation after it has commenced.

6.9 **Intrusive Surveillance** occurs when surveillance:

- is covert;
- relates to residential premises and 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.

Residential premises does not include common areas to which a person has access in connection with their use of occupation for example hotel reception area or communal stairways.

6.9.1 Directed surveillance carried out at the following locations for the purpose of legal consultation shall be treated as intrusive surveillance:

- any place in which persons who are serving sentences of imprisonment or detention, remanded in custody or committed in custody for trial or sentence may be detained;
- police stations;
- hospitals where psychiatric services are provided;
- the place of business of any professional legal adviser;
- any place used for the sittings and business of any court, tribunal, inquest or enquiry;
- any place which persons may be detained under certain circumstances provided by the Immigration Act 1971 or UK Border Act 2007.

Intrusive surveillance can be carried out only by police and other law enforcement agencies. **Council officers must not carry out intrusive surveillance.**

6.10 **'Covert human intelligence source' (CHIS)** is defined as a person who establishes or maintains a personal or other relationship with a person for the covert purpose of obtaining information or providing access to information to another person or covertly discloses information obtained through the use of such a relationship or as a consequence of the relationship.

6.11 **'Authorising Officer'** in the case of Local Authorities these are specified as Assistant Chief Officers (and more senior officers), Assistant Heads of Service, Service Managers or equivalent, responsible for the management of an investigation (see Regulation of Investigatory Powers (Directed Surveillance and Covert Human Intelligence Sources) Order 2010 (SI 2010/521). The Council's Authorising Officers are set out in Schedule 1 to this Policy.

6.12 **'Applicant Officer'** are those Council officers who apply for RIPA authorisation.

6.13 **'Crime Threshold'** applies to an authorisation for directed surveillance to prevent and detect conduct which constitutes one or more criminal offences. The criminal offences must be punishable, whether on summary conviction or indictment by a maximum term of at least 6 months imprisonment, or be an offence under:-

a) s.146 of the Licensing Act 2003 (sale of alcohol to children);
b) s.147 of the Licensing Act 2003 (allowing the sale of alcohol to children);
c) s.147A of the Licensing Act 2003 (persistently selling alcohol to children);
d) s.7 of the Children and Young Persons Act 1933 (sale of tobacco, etc, to persons under eighteen).

7.0 When does RIPA apply?

7.1 Where the directed covert surveillance of an individual or group of individuals, or the use of a CHIS is necessary for the purpose of preventing or detecting crime or of preventing disorder.

7.2 The Council can only authorise directed covert surveillance to prevent and detect conduct which constitutes one or more criminal offences. The criminal offences must be punishable, whether on summary conviction or indictment by a maximum term of at least 6 months imprisonment, or be an offence under:-

a) s.146 of the Licensing Act 2003 (sale of alcohol to children);
b) s.147 of the Licensing Act 2003 (allowing the sale of alcohol to children);
c) s.147A of the Licensing Act 2003 (persistently selling alcohol to children);
d) s.7 of the Children and Young Persons Act 1933 (sale of tobacco, etc, to persons under eighteen).

7.3 CCTV – the normal use of CCTV is not usually covert because members of the public are informed by signs that such equipment is in operation. However, authorisation should be sought where it is intended to use CCTV to target a specific individual or group of individuals via CCTV recordings may require authorisation (from the police).

7.4 The use of RIPA powers must be in relation to the performance of a core function of the Council and not 'ordinary functions' such as employment issues or contractual arrangements. It will include criminal misconduct investigations.

7.5 When considering the use of Social Media sites, RIPA may apply. If Social Media Sites are being accessed this should be done only by using a Council open account and generally to visit open source material only unless an authorisation is in place or the surveillance is overt. Even if open source sites are being accessed, the OSC has issued guidance as follows:

"Reviewing open source sites does not require authorisation unless the review is carried out with some regularity, usually when creating a profile, in which case directed surveillance authorisation will be required. If it becomes necessary to breach the privacy controls and become, for example "a friend" on the Facebook site, with the investigating officer utilising a false account concealing his/her identity as a council officer for the purpose of gleaning intelligence, this is a covert operation intended to obtain private information and should be authorised, at the minimum, as directed surveillance. If the investigator engages in any form of relationship with the account operator then s/he becomes a CHIS requiring authorisation as such and management by a controller and handler with a record being kept and a risk assessment created."

8.0 Training

8.1 Each Business Manager shall be responsible for ensuring that relevant members of staff, involved with any aspect of covert surveillance, are aware of the Act's requirements.

8.2 The Director of Safety shall ensure that refresher training is offered once a year to all services of the Council and also give advice and training on request. Applicant Officers must have received training or refresher guidance on RIPA within 2 years of the date of a request for RIPA authorisation.

9.0 Central Register and Records

9.1 A Central Register of all authorisations including the application for judicial approval, and Order form shall be retained within the Legal Services Business Unit. The content of the application forms and authorisations will be monitored to ensure that they comply with the Act. The Director of Safety will report any breaches of this Policy or the Act's provisions to the Corporate Management Team of the Council.

10.0 Overview and Scrutiny

10.1 The Director of Safety shall be the Senior Responsible Officer who will:

- ensure compliance with the Council's policy, relevant RIPA legislation and guidance;
- engage with Commissioners and inspectors when the Council's inspection is due (usually every three years);
- oversee any post-inspection action plans recommended or approved by a Commissioner.

10.2 This policy shall be reviewed, and where necessary amended, at least once a year. If requiring amendment, the revised policy shall be presented to and considered by the following:

- the Corporate Management Team
- the relevant Council Committee

10.3 The Senior Responsible Officer will report to the relevant Council committee, detailing the Council's use of RIPA powers, annually.

10.4 The Council's elected members will not be involved in any decisions made on specific authorisations granted.

GUIDANCE – PART I

DIRECTED SURVEILLANCE AND COVERT HUMAN INTELLIGENCE SOURCE

1.0 Covert Human Intelligence Source

1.1 Put simply, this means the use of, undercover officers or professional witnesses to establish or maintain a relationship with a person which is used to obtain information and evidence that you might not otherwise acquire.

1.2 The RIPA definition (section 26) is anyone who:-

a) establishes or maintains a personal or other relationship with a person for the covert purpose of facilitating the doing of anything falling within paragraphs b) or c);

b) covertly uses such a relationship to obtain information or provide access to any information to another person; or

c) covertly discloses information obtained by the use of such a relationship or as a consequence of the existence of such a relationship.

1.3 Any reference to the conduct of a CHIS includes the conduct of a source which falls within a) to c) or is incidental to it. References to the use of CHIS are references to inducing, asking or assisting a person to engage in such conduct.

1.4 Section 26(9) of RIPA goes on to define:-

b) a purpose is covert, in relation to the establishment or maintenance of a personal or other relationship if, and only if, the relationship is conducted in a manner that is calculated to ensure that one of the parties to the relationship is unaware of that purpose; and

c) a relationship is used covertly, and information obtained as mentioned in SS (8)(c) above and is disclosed covertly if, and only if, it is used or as the case may be disclosed in a manner that is calculated to ensure that one of the parties to the relationship is unaware of the use or disclosure in question.

1.5 The Council is only likely to use a CHIS in **very exceptional circumstances**, and advice should be sought from the Director of Safety or the Deputy Chief Executive before any authorisation is sought.

1.6 If the Director of Safety (or Deputy Chief Executive) deems that the use of a CHIS is appropriate the application must be authorised and judicial approval obtained.

1.7 The provisions of RIPA relating to CHIS do **not** apply:

a) where members of the public volunteer information to the Council as part of their normal civic duties;
b) where the public contact telephone numbers set up by the Council to specifically receive information;
c) where test purchases are carried out in the normal course of business;
d) where members of the public are asked to keep diaries of incidents in relation to planning enforcement or anti social behaviour.

as none of these situations normally require a relationship to be established for the covert purpose of obtaining information.

1.8 If a CHIS is used, both the use of the CHIS and his or her conduct require prior authorisation and judicial approval:

a) Conduct – establishing or maintaining a personal or other relationship with a person for the covert purpose of (or incidental to the covert purpose of) obtaining and passing on information
b) Use – inducing, asking or assisting a person to engage in the conduct of a source or to obtain information by means of the conduct of such a source.

1.9 One person within the Council should be responsible for tasking the source, dealing with them, directing their day-to-day activities and recording information supplied by them and monitoring their welfare and security. A risk assessment MUST be carried out at the start, during and after the investigation.

1.10 Special safeguards exist for the use of juvenile individuals who are under the age of 18 years old as a CHIS. The Regulation of Investigatory Powers (Juveniles) Order 2000 details the special provisions that should be satisfied.

1.11 Only the Chief Executive, or in his absence the Deputy Chief Executive, may grant an authorisation for the use of a juvenile as a CHIS. Under no circumstances may a juvenile under the age of 16 be authorised to act as a CHIS against the wishes of his parents or person who has parental responsibility for him. The duration of an authorisation for the use of a juvenile as a CHIS is one month.

1.12 A vulnerable individual is a person who is or may be in need of community care services for reason of mental or other disability, age or illness or is unable to take care of himself or protect himself from significant harm or exploitation. Only in the most exceptional circumstances may the Chief Executive, or in his absence the Deputy chief Executive, grant an authorisation for the use of a vulnerable individual as a CHIS.

1.13 There is a risk that an informant who is providing information to the Council voluntarily may in reality be a CHIS even if not tasked to obtain information covertly. It is the activity of the CHIS in exploiting a relationship which is authorised in the 2000 Act, not whether the CHIS is asked to do so by the Council. Where an informant gives repeat information about a suspect or about a family and it becomes apparent that the informant may be obtaining the information in the course of a neighbourhood or family relationship it may mean that the informant is in fact a CHIS. Legal advice should always be sought in such instances before acting on the information from any such informant.

2.0 Directed Surveillance

2.1 All application forms see http://www.homeoffice.gov.uk/counter-terrorism/regulation-investigatory-powers/ripa-forms/ must be fully completed by the Applicant Officer with the required details and sufficient information to enable the Authorising Officer to make an informed decision that he/she is satisfied and believes that RIPA is necessary and proportionate. The application form must also provide all the information required for approval by the Judiciary. No authorisation shall be granted unless the Authorising officer is satisfied that the RIPA authorisation is:

- Necessary for either the purpose of preventing or detecting crime or the prevention of disorder that involves a criminal offence or offences that are either punishable, whether on summary conviction or indictment, by a maximum term of at least six months imprisonment or are related to the underage sale of alcohol and tobacco (see paragraph 7.2 above);
- Proportionate this means that:
  - the method of surveillance proposed is not excessive to the seriousness of the matter under investigation;
  - it must be the method that is least invasive of the individual or individuals being observed;
  - the privacy of innocent members of the public must be respected and collateral intrusion minimised (see 2.2 below); and
  - that no other form of investigation would be appropriate.

The authorisation completed by the Authorising Officer should indicate that full consideration has been given to the above points and a record should be made on the appropriate forms.

Both the Applicant and Authorising Officers should refer themselves to their training notes regarding the completion of the RIPA forms, with particular attention to necessity and proportionality.

2.2 The Authorising Officer must also take into account the risk of **'collateral intrusion**' i.e. intrusion on, or interference with, the privacy of persons other than the subject of the investigation, particularly where there are special sensitivities e.g. premises used by lawyers, doctors or priests for any form of medical or professional counselling or therapy. The application form must include a detailed assessment of any risk of collateral intrusion for this purpose.

2.3 Steps must be taken to avoid unnecessary collateral intrusion and minimise any necessary intrusion. The applicant officer must inform the authorising officer of any unexpected interference with the privacy of individuals who are not covered by the authorisation, as soon as these become apparent.

2.4 A single authorisation may refer to a number of individuals but relate to a single investigation and are "same fact". However, necessity, proportionality and collateral intrusion should be considered individually. If particular subjects are subsequently ruled out of the investigation, those individuals could be removed at the next review. Such circumstances could prompt an early review.

2.5 Special consideration should be given in respect of confidential information. Particular attention is drawn to areas where the subject of surveillance may reasonably expect a high degree of privacy e.g. where confidential information is involved. Confidential information consists of matters subject to legal privilege, confidential personal information or confidential journalistic material (ss 98-100 Police Act 1997). The Chief Executive, or in his absence the Deputy Chief Executive, must sign any authorisation before judicial authority is sought.

2.5.1 Legal Privilege

This applies to Legal Consultation and includes communications or consultation between an individual and his/her legal adviser or a person representing their Client in connection with the giving of legal advice in connection with or in contemplation of legal proceedings. This also includes consultations with medical practitioners. Such information is unlikely ever to be admissible as evidence in criminal proceedings.

The advice of the Director of Safety must be sought in respect of any issues in this area.

2.5.2 Confidential Personal Information

This is oral or written information held in (express or implied) confidence, relating to the physical or mental health or spiritual counselling concerning an individual (alive or dead) who can be identified from it. Specific examples provided in the codes of practice are consultations between a health professional and a patient, discussions between a minister of religion and an individual relating to the latter's **spiritual welfare** or matters of **medical or journalistic confidentiality**.

2.5.3 Confidential Journalistic Material

This is material acquired or created for the purposes of journalism and held subject to an undertaking to hold it in confidence.

It should be noted that matters considered under RIPA may not necessarily be properly regarded as confidential under Section 41 Freedom of Information Act.

Where such information is likely to be acquired, the surveillance may only be authorised by the Chief Executive, or in his absence, the Deputy Chief Executive.

3.0 Judicial Approval of Authorisations

3.1 Once the Authorising Officer has authorised the Directed Surveillance of CHIS the Applicant Officer (who completed the application form) should contact the Magistrates' Court to arrange a hearing for the authorisation to be approved by a Justice of the Peace (JP).

3.2 The Applicant Officer will provide the JP with a copy of the original authorisation and the supporting documents setting out the case. This forms the basis of the application to the JP and should contain all the information that is relied upon.

3.3 In addition the Applicant Officer will provide the JP with a partially completed judicial application/order form.

3.4 The hearing will be in the Magistrates' Court and the Applicant Officer will be sworn in and present the evidence as required by the JP. Any such evidence should be limited to the information in the authorisation.

3.5 The JP will consider whether they are satisfied that at the time the authorisation was given there were reasonable grounds for believing that the authorisation or notice was necessary and proportionate and whether that continues to be so. They will also consider whether the authorisation was given by the appropriately designated person at the correct level within the Council and whether (in the case of directed surveillance) the crime threshold has been met.

3.6 Urgent authorisations should not normally be necessary. However, in exceptional circumstances, if the authorisation cannot be handled on the next working day the Court's out-of-hours service can be contacted. Legal Advice should be sought from the Director of Safety about whether it is appropriate to utilise this facility.

3.7 It will not be an urgent or exceptional circumstance where the need for authorisation has been neglected, or the situation is of the Applicant officer's own making.

3.8 The Justice of the Peace can:

a) Approve the grant of the authorisation which means that the authorisation will then take effect; or
b) Refuse to approve the grant of the authorisation which means the authorisation will not take effect but the Council may look at the reasons for the refusal, make amendments and re-apply for judicial approval; or
c) Refuse to approve the grant of the authorisation and quash the original authorisation. The Court cannot exercise its power to quash the authorisation unless the applicant has at least two business days from the date of the refusal in which to make representations.

4.0 Notifications to Inspector/Commissioner

4.1 The following situations must be brought to the Inspector/Commissioner's attention at the next inspection:

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

5.0 Applications for CHIS

5.1 The process is the same as for directed surveillance except that the authorisation must specify the activities and identity of the CHIS 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 http://www.homeoffice.gov.uk/counter-terrorism/regulation-investigatory-powers/ripa-forms/ must be fully completed with the required details to enable the Authorising Officer to make an informed decision and to be approved by the Judiciary.

6.0 Duration and Cancellation

6.1 Every authorisation and every renewal (except in the cases of oral authorisations or where the use of juvenile CHIS is being authorised) must be for the designated statutory period. If the operation is to only last for a short time, this is information which should be considered in the review and/or cancellation.

6.2 An authorisation for directed surveillance shall cease to have effect (if not renewed) 3 months less one day from the date of judicial approval but still requires to be cancelled using the appropriate form even if the surveillance is required for less than 3 months.

6.3 An authorisation for CHIS shall cease to have effect (unless renewed) 12 months from the date of judicial approval but it is still necessary to cancel the authorisation using the appropriate form.

NOTE:
The Applicant Officer authorised to carry out surveillance, in accordance with s.45 of the Act, must cancel each authorisation as soon as they decide that the surveillance should be discontinued. Authorisations should continue for the minimum period reasonable for the purpose they are given and then cancelled promptly.

7.0 Reviews

7.1 The Authorising Officer should review all authorisations prior to the expiry date and at intervals determined by him/herself. This should be as often as necessary and practicable. Particular attention should be paid to the possibility of obtaining confidential information. The Applicant Officer can do the necessary research and prepare the papers for the review but the actual review is the responsibility of the original Authorising Officer and should be conducted by him. Necessity and proportionality should be reconsidered if the surveillance is to continue.

7.2 The Authorising Officer should be made aware of any proposed or unforeseen changes to the nature or extent of the surveillance operation which may result in further or greater intrusion into the private life of any person by means of a review. The Authorising Officer should consider whether the proposed changes are proportionate before approving or rejecting them.

7.3 Where authorisation is given for surveillance of unidentified individuals whose identity is later established, the review should include reference to their identity. A fresh authorisation won't be necessary if the investigation remains the same.

7.4 Evidence of the review should be recorded.

8.0 Renewals

8.1 Any Authorising Officer may renew an existing authorisation on the same terms as the original at any time before the original ceases to have effect. This renewal must then be approved by a Justice of the Peace in the same way the original authorisation was approved. The process set out in 3 above should be followed.

8.2 A CHIS authorisation must be thoroughly reviewed before any application for renewal is sought. Once the Authorising Officer has approved an application to renew, that application must then be approved by a Justice of the Peace in the same way that the original authorisation was approved. The process set out in 3 above should be followed.

9.0 Central Register of Authorisations

9.1 The Council must maintain the following documents:

- Copy of the application and a copy of the authorisation together with any supplementary documentation and notification of the approval given by the authorised officer;
- Copy of the order made by the judiciary;
- 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 the authorisation;
- A copy of any renewal of an authorisation and order made by the judiciary and supporting documentation submitted when the renewal was requested;
- The date and time when any instruction was given by the Authorising Officer.

9.2 To comply with 9.1 above, the Council's RIPA Co-ordinating Officer within the Legal Services Business Unit will hold the central register of all authorisations issued by Authorising Officers of the Council. The original copy of every authorisation, judicial order, review, renewal and cancellation issued should be lodged immediately with Legal Services in an envelope marked 'Private and Confidential'.

9.3 The Council must also maintain a centrally retrievable record of the following information:

- Type of authorisation
- Date the authorisation was given
- Date the Order was made by the Justice of the Peace
- Name and rank/grade of the Authorising Officer
- Unique reference number of the investigation/operation
- Title (including brief description and names of the subjects) of the investigation/operation;
- Whether urgency provisions were used, and if so why
- Details of renewal
- Whether the investigation/operation is likely to result in obtaining confidential information
- Date of cancellation
- Confidential Information
- Self - Authorisation
- Reviews

These records will be retained for at least 3 years and will be available for inspection by the Office of Surveillance Commissioners.

10.0 Retention of Records

10.1 All documents must be treated as strictly confidential and the Authorising Officer must make appropriate arrangements for their retention, security and destruction, in accordance with the Council's Data Protection Policy and the RIPA codes of practice. The retention period for the purposes of this guidance is three years from the ending of the period authorised.

10.2 The Council's Records Retention and Disposal Policy should be referred to which sets out how different types of records are created as part of any investigation, their storage, retrieval, maintenance, protection and final disposal. The Council also has a separate Code of Practice which covers these issues specifically for CCTV tapes.

11.0 Complaints Procedure

11.1 The Council will maintain the standards set out in this guidance and the relevant Codes of Practice. The Chief Surveillance Commissioner has responsibility for monitoring and reviewing the way the Council exercises the powers and duties conferred by RIPA.

11.2 Contravention of the Data Protection Act 1998 may be reported to the Information Commissioner. Before making such a reference, a complaint concerning a breach of this guidance should be made using the Council's own internal complaints procedure. To request a complaint form, please contact Customer Services, Newark & Sherwood District Council, Kelham Hall, Kelham, Newark, Notts NG23 5QX or telephone 01636 650000.

GUIDANCE – PART II

ACQUISITION AND DISCLOSURE OF COMMUNICATIONS DATA

1.0 Acquisition and Disclosure of Communications Data

1.1 With effect from 5 January 2004, and in accordance with Chapter II of Part I of Regulation of Investigatory Powers Act ("the Act"), Local Authorities can authorise the acquisition and disclosure of 'communications data' provided that the acquisition of such data is necessary for the purpose of preventing or detecting crime or preventing disorder; and proportionate to what is sought to be achieved by acquiring such data.

Important: The Council is not Permitted to Intercept any Communications

1.2 The procedure is similar to that of authorisation for directed surveillance and CHIS but has extra provisions and processes. The purpose and effect of the procedure is the same i.e. to ensure proper consideration is given to permitting such investigations and to provide protection against a human rights challenge. The Authorising Officer is called a 'Designated Person'. Judicial approval for the acquisition and disclosure of communications data is required.

2.0 What is 'Communications Data'?

2.1 Communications Data is information relating to the use of a communications service e.g. postal service or telecommunications system. It is defined by Section 21(4) of the Act and falls into three main categories:-

Traffic Data

Where a communication was made from, to whom and when.

Service Data

Use made of service e.g. itemised telephone records.

Subscriber Data

Information held or obtained by operator on person they provide a service to.

Local Authorities are restricted to subscriber and service use data and only for the purpose of preventing or detecting crime or preventing disorder.

3.0 Designated Person

3.1 A Designated Person must be at least the level of Director or equivalent. Details of the Council's Designated Persons are included in Schedule 1.

4.0 Application Forms

4.1 All applications must be made on a standard form (see http://www.homeoffice.gov.uk/counter-terrorism/regulation-investigatory-powers/ripa-forms/).

5.0 Authorisations

5.1 Authorisations can only authorise conduct to which Chapter II of Part I of the Act applies. In order to comply with the code, a Designated Person can only authorise the obtaining and disclosure of communications data if:

i) It is **necessary** for any of the purposes set out in Section 22(2) of the Act. (NB The Council can only authorise for the purpose set out in Section 22(2)(b) which is the purpose of preventing or detecting crime or preventing disorder); and

ii) It is **proportionate** to what is sought to be achieved by the acquisition of such data (in accordance with Section 22(5) the Act).

Consideration must also be given to the possibility of collateral intrusion and whether any urgent timescale is justified.

5.2 Once a Designated Person has decided to grant an authorisation or a notice and judicial approval has been granted there are two methods:-

i) By authorisation of some person in the same relevant public authority as the Designated Person, whereby the relevant public authority collects the data itself (Section 22(3) the Act). This may be appropriate in the following circumstances:

- The postal or telecommunications operator is not capable of collecting or retrieving the communications data;
- It is believed the investigation may be prejudiced if the postal or telecommunications operator is asked to collect the data itself;
- There is a prior agreement in place between the relevant public authority and the postal or telecommunications operator as to the appropriate mechanisms for the disclosure of communications data.

ii) By notice to the holder of the data to be acquired (Section 22(4)) which requires the operator to collect or retrieve the data. Disclosure may only be required to either the designated person or the single point of contact.

5.3 The Service provider must comply with the notice if it is reasonably practicable to do so (S.22 (6)-(8) and can be enforced to do so by civil proceedings. The postal or telecommunications service can charge for providing this information. There are standard forms see http://www.homeoffice.gov.uk/counter-terrorism/regulation-investigatory-powers/ripa-forms/ for authorisations and notice.

6.0 Oral Authority

6.1 The Council is not permitted to apply or approve orally.

7.0 Single Point of Contact (SPOC)

7.1 Notices and authorisations should be passed through a single point of contact within the Council. This should make the system operate more efficiently as the SPOC will deal with the postal or telecommunications operator on a regular basis and also be in a position to advise a Designated Person on the appropriateness of an authorisation or notice.

7.2 SPOCs should be in a position to:

- Where appropriate, assess whether access to communication data is reasonably practical for the postal or telecommunications operator;
- Advise applicants and designated person on whether communications data falls under Section 21(4)(a), (b) or (c) of the Act;
- Provide safeguards for authentication;
- Assess any cost and resource implications to both the public authority and the postal or telecommunications operator.

7.3 A SPOC must be accredited which involves undertaking appropriate training. The Council currently has no SPOC and does not currently envisage circumstances where it would be necessary for the Council to authorise the acquisition and disclosure of communications data. However, this aspect of the Policy will be regularly reviewed.

8.0 Duration

8.1 Authorisations and notices are only valid for one month beginning with the date on which the judicial approval is granted or the notice given. A shorter period should be specified if possible.

9.0 Renewal and Cancellation

9.1 An authorisation or notice may be renewed at any time during the month it is valid using the same procedure as used in the original application (including seeking judicial approval). A renewal takes effect on the date which the authorisation or notice it is renewing expires.

9.2 The code requires that all authorisations and notices should be cancelled by the Designated Person who issued it as soon as it is no longer necessary, or the conduct is no longer proportionate to what is sought to be achieved. The relevant postal or telecommunications operator should be informed of the cancellation of a notice.

10.0 Retention of Records

10.1 Applications, authorisations and notices must be retained until the Council has been audited by the Commissioner (see paragraph 9). Applications must also be retained to allow the Tribunal (see paragraph 9) to carry out its functions.

10.2 A record must be kept of:-

- The dates of which the authorisation or notice is started or cancelled;
- Any errors that have occurred in the granting of authorisations or giving of notices.

A report and explanation of any errors must also be sent to the Commissioner as soon as is practicable. Communications data, and all copies, extracts and summaries of it, must be handled and stored securely and the requirements of the Data Protection Act 1998 must be observed. The Director Safety will maintain a centrally retrievable register.

11.0 Oversight and Complaints

11.1 The Act provides for an Interception of Communications Commissioner whose remit is to provide independent oversight of the use of the powers contained in Part I and the code requires any person who uses the powers conferred by Chapter II to comply with any request made by the Commissioner to provide any information he requires to enable him to discharge his functions.

11.2 The Act also establishes an independent Tribunal to investigate and decide any case within its jurisdiction. Details of the relevant complaints procedure should be available for reference at The Council's public offices.

SCHEDULE 1

Designated Persons/Authorising Officers

Chief Executive
Deputy Chief Executive

Note: When the above are the Applicant Officer in a matter they may NOT authorise the same application for surveillance.

Senior Responsible Officer

Director – Safety

RIPA Co-ordinating Officer

Senior Legal Officer – Caroline O'Hare