REGULATION OF INVESTIGATORY POWERS ACT 2000 (RIPA) POLICY

GEDLING BOROUGH COUNCIL

REGULATION OF INVESTIGATORY POWERS ACT 2000 (RIPA)

POLICY

CONTENTS

Page nos.

Appendices

GEDLING BOROUGH COUNCIL

POLICY ON REGULATION OF INVESTIGATORY POWERS ACT 2000

Introduction

Gedling Borough Council ("the Council") only carries out covert surveillance or utilises covert human intelligence sources where such action is justified and endeavours to keep such activities to a minimum. It recognises its obligation to comply with the Regulation of Investigatory Powers Act 2000 ("RIPA/the Act") when such an investigation is for the purpose of preventing or detecting crime or preventing disorder, and has produced this guidance document to assist officers.

Applications for authority

An officer of at least the level of Director will act as Authorising Officer and consider all applications for authorisation in accordance with RIPA. Any incomplete or inadequate application forms will be returned to the applicant for amendment. The Authorising Officer shall in particular ensure that: -

- **there is a satisfactory reason for carrying out the covert technique**
- **any directed surveillance passes the "serious crime" threshold**
- **the covert nature of the investigation is necessary for the prevention and detection of crime or preventing disorder**
- **proper consideration has been given to collateral intrusion**
- **the proposed length and extent of the RIPA activity is proportionate to the information being sought.**
- **Chief Executive's authorisation is sought where confidential legal/medical/clerical/parliamentary/journalistic/ spiritual welfare issues are involved or a juvenile covert human intelligence source is proposed.**
- **The authorisations are reviewed and cancelled.**
- **Records of all authorisations are sent to Legal Services for entry on the Central Register.**

Once authorisation has been obtained from the Authorising Officer the Authorising Officer will attend the Magistrates' Court in order to obtain Judicial approval for the authorisation.

Training

Each Authorising Officer shall be responsible for ensuring that relevant members of staff are aware of the Act's requirements.

The ~~Head of Governance and Customer Services~~Deputy Chief Executive shall ensure that refresher training is offered once a year to all directorates of the Council and also give advice and training on request.

Central register and records.

Legal Services shall retain the Central Register of all authorisations issued by the Council. Legal Services will also monitor the content of the application forms and authorisations to ensure that they comply with the Act.

Senior Responsible Officer ("SRO")

The Senior Responsible Officer, a role required by the Investigatory Powers Commissioner (the "IPC") with oversight of the Council's use of RIPA powers is the ~~Head of Governance and Customer Services~~Deputy Chief Executive.

RIPA Co-ordinating Officer

The RIPA Co-ordinating Officer role, with the responsibility for the day to day RIPA management and administrative processes observed in obtaining an authorisation and advice thereon, is performed by the ~~Senior Legal Officer - Litigation and Licensing~~Legal Services Manager.

REGULATION OF INVESTIGATORY POWERS ACT 2000 (RIPA)

GUIDANCE ON PART II

DIRECTED SURVEILLANCE AND COVERT HUMAN INTELLIGENCE SOURCE

1. Purpose

The purpose of this guidance is to explain

the scope of RIPA –Part II
the circumstances where it applies, and
the authorisation procedures to be followed.

2. Introduction

2.1 This Act, which came into force in 2000, is intended to regulate the use of investigatory powers exercised by various bodies including local authorities, and ensure that they are used in accordance with human rights. This is achieved by requiring certain investigations to be authorised by an appropriate officer and approved by the judiciary before they are carried out.

2.2 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 6 month' 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 are attached at **Appendix B.**

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

3. Scrutiny and Tribunal

3.1 External

3.1.1 As of 1st November 2012 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 carried out. The Council can only appeal a decision of the Justice of the Peace on a point of law by Judicial review.

3.1.2 The Investigatory Powers Commissioner ("IPC"), a role established by the Investigatory Powers Act 2016 has comprehensive oversight of the use of RIPA powers by public authorities and will ensure compliance with the law by inspecting public authorities and investigating any issue which they believe warrant further scrutiny. The IPC will have unfettered access to all locations, documentation and information systems necessary to carry out their full functions and duties.

3.1.3 In order to ensure that investigating authorities are using the powers properly, the Act also establishes the Investigatory Powers Tribunal, a Tribunal to hear complaints from persons aggrieved by conduct, e.g. directed surveillance. 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.

3.1.4 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.

3.1.5 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

3.2 Internal scrutiny

3.2.1 The Council will ensure that the SRO is responsible for;

- The integrity of the process in place within the Council to authorise directed surveillance and CHIS
- Compliance with PART II of the 2000 Act and with the accompanying Codes of Practice
- Engagement with the Commissioner and inspectors when they conduct their inspections and
- Where necessary overseeing the implementation of any post-inspection action plans recommended or approved by the Commissioner

3.2.2 The elected members of the Council will review the Council's use of the Act and the Council's policy and guidance documents at least once a year. Members will also consider internal reports on a regular basis throughout the year indicating the nature of RIPA activity undertaken or inactivity, to ensure that any use is consistent with the Council's policy and that the policy is fit for purpose. The members will not however be involved in making decisions on specific authorisations.

3.3 Unauthorised Activities

3.3.1 If any Officer is concerned that surveillance/CHIS activity is taking place and there is no authorisation under RIPA in place, he/she should contacted Legal Services to seek advice.

3.3.2 If any activity is deemed to be unauthorised, it will be reported to the IPC.

4. Benefits of RIPA authorisations

4.1 The Act states that if authorisation confers entitlement to engage in a certain conduct and the conduct is in accordance with the authorisation, then it will be lawful for all purposes. Consequently, RIPA provides a statutory framework under which covert surveillance or CHIS can be authorised and conducted compatibly with Article 8 of the Human Rights Act 1998 – a person's right to respect for their private and family life, home and correspondence.

4.2 Material obtained through properly authorised covert activity is admissible evidence in criminal proceedings.

5. Definitions

5.1 'Covert' is defined as surveillance carried out in such a manner that is calculated to ensure that the person subject to it is unaware that it is or may be taking place. (s.26 (9)(a))

5.2 '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 process of obtaining/providing access to/disclosing, information obtained through that relationship or as a consequence of the relationship(s.26 (8))

5.3 'Directed surveillance' is defined as covert but not intrusive surveillance and undertaken:

- for a specific investigation or operations,
- in such a way that is likely to result in the obtaining of private information about any person,
- other than by way of an immediate response.(s.26 (2))

5.4 'Private information' includes any information relating to a person's private or family life (s.26(10)). Private information should be taken generally to include information on any aspect of a person's private or personal relationship with others including family and professional or business relationships. It is likely to be the case that where a person has a reasonable expectation of privacy, even though acting in public or placing information on publicly accessible areas of the internet, and where a record of that activity is being made by a

public authority of that person's activities for future consideration or analysis, that this will result in obtaining private information.

5.5 'Intrusive' surveillance is covert surveillance that is carried out in relation to anything taking place on any residential premises or in any private vehicle and involves the presence of an individual on the premises or in the vehicle or using a surveillance device. **Gedling Borough Council cannot authorise such surveillance**. Residential premises do not include the front driveway or garden of a premises readily visible to the public, or a communal stairway in a block of flats.

5.6 'Authorising Officer' in the case of the Council, is the Chief Executive and Directors. If the operation concerns more than one department in the Council it can only be authorised by the Chief Executive.

6. When does RIPA apply?

6.1 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.

6.2 The Council can only authorise **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)

6.3 Core Functions

A public authority may only seek authorisations under the Act when in performance of its "core functions". Core functions are the specific public functions undertaken by the authority in contrast to the ordinary functions which are those undertaken by all authorities for example employment issues or contractual arrangements. The disciplining of an employee is not a core function, although related criminal investigations may be.

6.4 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 covertly and in a pre-planned manner as part of a specific investigation or operation to target a specific individual or group of individuals. Equally a request, say by

the police, to track particular individuals via CCTV recordings may require authorisation (from the police). Guidance on the operation of CCTV generally is provided in the Surveillance Camera Code of Practice issued under the Protection of Freedoms Act 2012, the Information Commissioner has also issued a code "In the Picture – A Data Protection Code of Practice for Surveillance Cameras and Personal Information", which authorities should have regard to.

6.5 Online Covert Activity

The use of the internet and social media sites may be required to gather information prior to and during an operation/investigation. Officers should exercise caution when utilising such sites during an investigation and be alert to situations where authorisations under RIPA may be required. If officers have any concerns over the use of social media during an investigation they should contact Legal Services. As a general rule of thumb however, reviewing open source sites such as facebook pages where no privacy settings are in place does not require an authorisation under RIPA unless review is carried out with some regularity, often to build a profile, when directed surveillance authorisation may be required.

Use of the internet prior to an investigation should not normally engage privacy considerations but if the study of an individual's online presence becomes persistent, or where material obtained from any check is to be extracted and recorded and may engage privacy considerations, a RIPA authorisation may be required. If the officer then, for the purposes of gleaning intelligence breaches privacy controls and becomes for example a "friend" within a subject's facebook account, utilising a pseudo account to conceal his/her identity as a Council official, this is a covert operation which, by its nature, is intended to obtain private information and should be authorised as a minimum as directed surveillance. Further, if the officer engages in any form of relationship with the account operator then s/he is likely to become a CHIS requiring authorisation and management by a Controller and Handler with a record being kept and a risk assessment created.

In deciding whether online surveillance should be regarded as covert, consideration should be given to the likelihood of the subject knowing that surveillance is or may be taking place. This is regardless of what privacy settings the individual may have in place.

7. Covert Human Intelligence Source

7.1 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

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 a CHIS are references to inducing, asking or assisting a person to engage in such conduct.

7.2 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.

7.3 With any authorised use of a CHIS, the Council must ensure that arrangements are in place for the proper oversight and management of the CHIS, this includes appointing individual officers as handlers and controllers in relation to the CHIS (s.29(5)(a) and (b)). The handler should not be the Authorising Officer. Appropriate risk assessments should also be prepared in relation to the CHIS activity.

7.4 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 for a covert purpose which is ultimately authorised in the 2000 Act, not whether or not the CHIS is asked to do so by the Council. When 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 any information from such an informant.

7.4 Juvenile Sources

7.4.1 Special safeguards apply to the use or conduct of juvenile sources; that is sources under the age of 18 years. On no occasion should the use or conduct of a source under the age of 16 years be authorised to give information against his parents or any person who has parental responsibility for him. The duration of a juvenile CHIS is **four** months. The Regulation of Investigatory Powers (Juveniles) Order 2000 contains special provisions which must be

adhered to in respect of juvenile sources. Any authorisation of a juvenile CHIS must be by the Chief Executive.

7.5 Vulnerable Individuals

7.5.1 A vulnerable individual is a person who by reason of mental disorder or vulnerability or other disability, age or illness is, or may be, unable to take care of himself, or unable to protect himself against significant harm or exploitation. Any individual of this description should only be authorised to act as a source in the most exceptional circumstances. Any authorisation of a vulnerable individual as a CHIS must be by the Chief Executive.

8. Authorisations

8.1 Applications for directed surveillance

8.1.1 All application forms must be fully completed with the required details to enable the authorising officer to make an informed decision. Application forms are available on the Home Office website, officers should ensure they are using the most up to date forms for RIPA authorisations. The authorisation will only commence on the date Magistrates Court approval is obtained (see 8.3) and runs for three months from that date of that approval.

No authorisation shall be granted unless the authorising officer is satisfied that the investigation is:

-**necessary** for either the purpose of preventing or detecting crime or of preventing disorder,

-Involves a criminal offence punishable whether summarily or on indictment by a maximum sentence of at least six months imprisonment or related to the underage sale of alcohol or tobacco (see para 6.2 for offences)

-**proportionate** and this has 4 elements, namely:
(1) that the method of surveillance proposed is not excessive to the seriousness of the matter under investigation,
(2) the method used must be the least invasive of the target's privacy,
(3) the privacy of innocent members of the public must be respected and collateral intrusion minimised (see 8.1.2).
(4) that no other form of investigation would be appropriate. This should be evidenced by explaining what other methods of investigation have been considered or tried and why they have not been implemented or why they failed.

The grant of authorisation should indicate that consideration has been given to the above points.

Advice should be sought from the Legal Services on any issues of concern.

8.1.2 The Authorising Officer must take into account the risk of obtaining private information about persons who are not subjects of the surveillance activity -**'collateral intrusion'** i.e. intrusion on, or interference with, the privacy of persons other than the subject of the investigation. The application must include an assessment of any risk of collateral intrusion for this purpose.

Steps must be taken to avoid unnecessary collateral intrusion and minimise any necessary intrusion.

Those carrying out the investigation must inform the Authorising Officer of any unexpected interference with the privacy of individuals who are not covered by the authorisation, as soon as it becomes apparent. Where such collateral intrusion is unavoidable, the activities may still be authorised, provided this intrusion is considered proportionate to what is sought to be achieved. The same considerations in respect of proportionality outlined in para 8.1.1 apply to the assessment of collateral intrusion.

The Authorising Officer should also fully understand the capabilities and sensitivity levels of any equipment being used to carry out directed surveillance so as to properly assess the risk of collateral intrusion in surveillance techniques.

8.1.3 Special consideration in respect of confidential information

Particular attention is drawn to areas where the subject of surveillance may reasonably expect a high degree of privacy eg where confidential information is involved.

Confidential information consists of matters subject to legal privilege, communication between a Member of Parliament and another person on constituency matters, confidential personal information or confidential journalistic material, or where material identifies a journalist's source. (ss 98-100 Police Act 1997).

Legal privilege

Generally, this applies to communications between an individual and his/her legal adviser in connection with the giving of legal advice in connection with or in contemplation of legal proceedings. Such information is unlikely ever to be admissible as evidence in criminal proceedings.

If in doubt, the advice of Legal Services should be sought in respect of any issues in this area.

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 of 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

Confidential constituent information

This is information relating to communication between a Member of Parliament and a constituent in respect of constituency business. Such information is held in confidence if it is held subject to an express or implied undertaking to hold it in confidence or it is subject to a restriction on disclosure or an obligation of confidentiality contained in existing legislation.

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. There is a strong public interest in protecting a free press including the willingness of sources to provide information to journalists in confidence.

It should be noted that matters considered to be confidential under RIPA may not necessarily be properly regarded as confidential under section 41 Freedom of Information Act 2000.

Where such information is likely to be acquired, the surveillance may only be authorised by the Chief Executive, or, in his absence, a Chief Officer and should only be authorised where there are exceptional and compelling circumstances that make the authorisation necessary.

8.1.4 Authorisations must be in writing and have a "wet" signature .

8.1.5 Notifications to Inspector/Commissioner

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.

8.2 Applications for CHIS

The process for CHIS applications is the same as for directed surveillance except that the serious crime threshold of investigating criminal offences with a sentence of at least 6 months in imprisonment does not apply. The authorisation must be in writing, must specify the activities and identity (by pseudonym only) 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.

Again the Authorising Officer must be satisfied that the authorised use and conduct of the CHIS is proportionate to what is sought to be achieved by that conduct and the CHIS must be necessary for the prevention or detection of crime or the prevention of disorder. Collateral intrusion must also be considered.

All application forms must be fully completed with the required details to enable the Authorising Officer to make an informed decision. A risk assessment and record must be prepared for each CHIS.

8.3 Judicial Approval of authorisations (see guidance at Appendix C and D)

Once the Authorising Officer has authorised the Directed Surveillance or CHIS, the Authorising Officer who gave the authorisation should attend the Magistrates Court for the authorisation to be approved by a Justice of the Peace. The hearing should ideally be on the same day as the Authorising Officer gives authorisation, the court should be contacted prior to attendance to ensure the matter can be heard.

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

In addition, the Authorising Officer will provide the Justice of the Peace with a partially completed judicial application/order form. These documents should be taken to the court by the Authorising Officer and not sent to the court my any other means prior to the hearing.

The hearing will be in private and the Authorising Officer will be sworn in and present evidence as required by the Justice of the Peace. Any such evidence should be limited to the information in the authorisation.

The Justice of the Peace will consider whether he/she is 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 the case. They will also consider whether the authorisation was given by the appropriate designated person at the correct level within the Council and whether (in the case of directed surveillance) the crime threshold has been met.

The Justice of the Peace can :

a) **Approve the grant of the authorisation** ,which means the authorisation will then take effect for a period of three months.
b) **Refuse to approve the grant of the authorisation**, which means the authorisation will not take effect but the Council could look at the reasons for refusal, make any amendments and reapply for judicial approval.
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 2 business days from the date of the refusal in which to make representations.

8.4 **Working in partnership with the Police/Collaborative Working**

Authorisation can be granted in situations where the police rather than Gedling Borough Council require the surveillance to take action, as long as the behaviour complained of, meets all criteria to grant and in addition is also of concern to the Council. Authorisation cannot be granted for surveillance requested by the police for a purely police issue.

The Police, as an emergency service may authorise RIPA without Magistrates approval, if an urgent situation arises and RIPA authorisation would be required urgently, the Council should contact the police if surveillance is deemed to be necessary and proportionate in an urgent situation.

Any person granting or applying for an authorisation will also need to be aware of particular sensitivities in the local community where the surveillance is taking place and of any other similar activities being undertaken by other public authorities which could impact on the deployment of surveillance or property interference. Where an Authorising Officers considers conflicts may arise they should consult a senior officer within the police.

Where the Police are carrying out surveillance and request the use of the Council's cameras to do so, the police should obtain the authorisation and provide sufficient information to the Council to enable the surveillance to be undertaken in line with the authorisation.

9. Unique Operation Reference Number

Each Application for Directed Surveillance and CHIS, must have a Unique Operation Reference Number. This URN will begin with either ENV (if it is granted in the Environment and Planning Department) or FIN (if it is granted in the Finance Department), followed by a sequential number, followed by 20?? being the year in which the Authority was applied for, e.g. ENV/27/2005

10. Duration and Cancellation

- An authorisation for **directed surveillance** shall cease to have effect (if not renewed or cancelled) 3 months from the date the Justice of the Peace approves the grant.

- If renewed, the authorisation shall cease to have effect 3 months from the expiry date of the original authorisation.

- An authorisation for **CHIS** shall cease to have effect (unless renewed or unless juvenile) 12 months from the date the Justice of the Peace approves the grant or renewal.

This does not mean that the authorisation should continue for the whole period so that it lapses at the end of this time. The Authorising Officer must cancel the authorisation at anytime if they consider the surveillance or CHIS no longer meets the criteria on which it was authorised.

On cancellation, the cancellation form should detail what product has been obtained as a result of the surveillance activity. The forms should include the dates and times of the activity, the nature of the product obtained and its format, any associated log or reference numbers, details of where the product is to be held and the name of the officer responsible for its future management.

Documentation of any instruction to cease surveillance should be retained and kept with the cancellation form.

11. Reviews

The Authorising Officer should review all authorisations at intervals determined by him/herself. This should be as often as necessary and practicable-usually monthly, however reviews may be more frequent where there is a high level of intrusion into a subject's private life or there is significant collateral intrusion. **The reviews should be recorded.**

If the directed surveillance authorisation provides for the surveillance of unidentified individuals whose identity is later established, the terms of the authorisation should be refined at review to include the identity of these

individuals. It would be appropriate to call a review specifically for this purpose**.**

Any changes to the nature or extent of the surveillance activity which results in a greater intrusion into the private life of any person should be raised at review and consideration of the necessity and proportionality test should be undertaken before any changes are approved or rejected.

Particular attention should be paid to the possibility of obtaining confidential information and an assessment as to the information gleaned should take place at every review.

12. Renewals

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. The renewal must then be approved by the Justice of the Peace in the same way the original authorisation was approved. The process outlined in paragraph 8.3 should be followed for renewals.

A CHIS authorisation must be thoroughly reviewed before it is renewed.

13. Central Register of authorisations

13.1 All authorities must maintain the following documents:

- Copy of the application and a copy of the authorisation form and the approval order from the Magistrates together with any supplementary documentation
- 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 Magistrates Court and supporting documentation submitted when the renewal was requested;
- The date and time when any instruction to cease surveillance as given
- The date and time when any other instruction was given by the Authorising Officer

13.2. To comply with 13.1 Legal Services hold the central register of all authorisations issued by officers of Gedling Borough Council. The original authorisation, reviews, renewal and cancellation issued should be passed immediately to Legal Services. A copy should be kept by the applicant Department and the Authorising Officer. Any original authorisations and

renewals taken to the Magistrates Court should be retained by the Council, the court must only keep copies of the authorisations or renewals.

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

- type of authorisation
- date the authorisation was given
- details of attendance at the Magistrates' Court, the date of the attendance, the determining Justice of the Peace, the decision of the court and the time and date of the decision
- 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;
- details and dates of reviews
- dates of any renewals including the name and rank of the Authorising Officer
- whether the investigation/operation is likely to result in obtaining confidential information
- whether the authorisation was granted by an individual directly involved in the investigation
- date of cancellation
- detail of any material obtained through surveillance with dates for review and destruction of such material

These records will be retained for at least 3 years and will be available for inspection by the IPC.

Where the Council has worked collaboratively with the Police and provided assistance on any police obtained RIPA authorisation such as utilising Council cameras for police surveillance, records of that activity should be retained including the instruction from Police and details of the authorisation.

14. Retention of records

The Council must ensure that arrangements are in place for the secure handling, storage and destruction of material obtained through the use of directed surveillance or CHIS. The Authorising Officers through their relevant Data Controller must ensure compliance with the appropriate data protection requirements under the General Data Protection Regulation ("GDPR") Data Protection Act 2018 and any relevant codes of practice relating to the handling and storage of material, in addition consideration should be given to the Council's Record Retention and Disposal Policy in relation to how long material from a RIPA authorisation is retained.

The Central Register of Authorisations will be kept securely in a locked cabinet in the Legal Services department. The Register will provide dates for

review and destruction of any RIPA material obtained as part of an authorised covert surveillance operation.

15. Complaints procedure

15.1 The Council will maintain the standards set out in this guidance and the Codes of Practice (**See Appendix B**). The Investigatory Powers Commissioner has responsibility for monitoring and reviewing the way the Council exercises the powers and duties conferred by RIPA.

15.2 Contravention of RIPA may be reported to the Investigatory Powers Tribunal. 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 make a complaint, please follow this link http://www.gedling.gov.uk/council/aboutus/complaintsandcompliments/complaints/ or contact us at Gedling Borough Council, Arnot Hill Park, Arnold Nottingham NG5 6LU on 0115 9013901.