Regulation of Investigatory Powers Act 2000 (RIPA)

**Corporate Policy and Procedures Guide** 

#### **Contents**

- A. Introduction
- **B. Policy Statement**
- C. Definitions
- D. General Information on RIPA
- E. The scope of RIPA
- F. Principles of RIPA Necessary and Proportionate
- G. Collateral Intrusion
- H. Surveillance
- I. Handling Product from Surveillance Activities
- J. Conduct and use of a Covert Human Intelligence Source (CHIS)
- K. Authorisation Procedures
- L. Information for Applicants/Requesting Officers
- M. Records Management

# A. INTRODUCTION

- 1. This document sets out the policies and procedures adopted by the Council to address the requirements of:
- (a) the Regulation of Investigatory Powers Act 2000 (RIPA) as amended by the Protection of Freedoms Act 2012 and the Regulations made under it;
- (b) the Home Office's Codes of Practices in relation to the Covert Surveillance of Individuals, the use of Covert Human Intelligence Sources (CHIS), including undercover officers, agents and informants (under Part II of RIPA) and on the judicial approval process for RIPA and the crime threshold for directed surveillance;
- (c) the guidance issued by the Office of Surveillance Commissioners; and
- (d) other associated relevant legislation
- 2. RIPA and this guide are important for the effective and efficient operation of the Council's investigations undertaken in relation to the exercise of its functions where these might involve covert surveillance and Covert Human Intelligence Sources.
- 3. If staff are in any doubt on RIPA, any related legislative provisions, this guide or any other related documentation, they should consult either the Audit Department, Monitoring Officer or Legal Department at the earliest possible opportunity and, certainly, before undertaking any enforcement activities.

# **B. POLICY STATEMENT**

- 4. The Council takes its statutory responsibilities seriously and will, at all times, act in accordance with the law and take necessary and proportionate action in these types of matters.
- 5. The Council has resolved that:
- All exercises relating to covert surveillance and the use of Covert Human Intelligence Sources must comply with the requirements of RIPA
- Only the specified grades of officers shall be permitted to authorise such exercises
- This guide and other related documentation shall be made available to all relevant staff that may carry out such exercises

6. The Monitoring Officer, and the Director of Resources are responsible for maintaining a continuous review of the RIPA Policy and submitting any additions or changes necessary to the Executive for approval.

3

#### C. DEFINITIONS

# **Authorising Officer**

Means the person(s) designated under Sections 28 and 29 of the Act to grant authorisations for directed surveillance and the use and conduct of a Covert Human Intelligence Source, respectively. Within each department, such officers should be documented and be in accordance with The Regulation of Investigatory Powers Act (Directed Surveillance and Covert Human Intelligence Sources) Order 2010 which prescribes that authorisations be granted byDirectors, Heads of Service and Service Managers or equivalent.

# **Confidential Material**

This includes: Matters of legal privilege; Confidential personal information (e.g. medical records); Confidential journalistic material.

# Matters Subject to Legal Privilege

Includes both oral and written communications between a professional legal adviser and his/her client or any person representing his/her client, made in connection with the giving of legal advice to the client or in contemplation of legal proceedings and for the purposes of such proceedings, as well as items enclosed with or referred to in such communications. Communications and items held with the intention of furthering a criminal purpose are not matters subject to legal privilege.

# Confidential Journalistic Material

Includes material acquired or created for the purposes of journalism and held subject to an undertaking to hold it in confidence, as well as communications resulting in information being acquired for the purposes of journalism and held subject to such an undertaking.

# **Covert Human Intelligence Source (CHIS)**

Commonly known as an Agent, Informant,or Undercover Officer this is someone who establishes or maintains a personal or other relationship (this must be a relationship and not a conversation) with a person for the covert purpose of obtaining information.

#### **Covert Surveillance**

Means surveillance carried out in a manner calculated to ensure that the persons subject to the surveillance are unaware that it is taking place (Section 26(9) (a) of RIPA). It can be either Directed or Intrusive.

#### **Directed Surveillance**

Is surveillance which is covert but not intrusive and which is undertaken for the purpose of a specific investigation or specific operation in such a manner as is likely to result in obtaining 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 may only be undertaken in the investigation of a criminal offence attracting a criminal sentence of not less than 6 months imprisonment or the investigation of offences relating to the sale of alcohol or tobacco to children.

#### **Intrusive Surveillance**

Means covert surveillance carried out in relation to anything taking place on residential premises or in a private vehicle. This kind of surveillance may take place by means of either a person or device located inside residential premises or a private vehicle of the person who is subject to the surveillance or by means of a device placed outside which consistently provides a product of equivalent quality and detail as a product which would be obtained from a device located inside. Local authorities are not authorised to conduct Intrusive Surveillance

#### **Private Information**

In relation to a person this includes any information relating to his/her private or family life, his home and his correspondence. It is important to remember that the Act is drafted in terms of the likelihood of obtaining private information rather than the intention to obtain it or about specific persons. Judgments from The European Court on Human Rights have concluded that private information includes what happens in the home, family and private life .but does not cover business or commercial activities.

#### **Communication Data**

This is information relating to electronic communications and falls into 3 types:

Traffic data – where communications were made or received

Service Use Information – the type of communication, time sent and duration Subscriber Information – this includes billing information such as the name address and bank details of the subscriber of telephone or internet services.

A Local Authority may authorise the acquisition of service use and subscriber information but not traffic data.

A Local Authority may not intercept the content of anyone's communications and it is a criminal offence to do so without lawful authority.

#### Controller

Means the person or designated managerial officer responsible for overseeing the use of the CHIS.

# Handler

An investigating officer having day to day responsibility for:

- Dealing with the CHIS on behalf of the authority
- · Directing the day to day activities of the CHIS
- Recording the information supplied by the CHIS
- Monitoring the security and welfare of the CHIS

#### **Conduct of a Source**

Any action of that CHIS, falling within the terms of the Act, or action incidental to it (i.e. What they do).

# Surveillance

Monitoring, observing or listening to persons, their movements, conversations, other activities or communications, recording anything monitored, observed or listened to in the course of surveillance and surveillance with a surveillance device (which means anything designed or adapted for surveillance use).

#### "The Use" of a Source

Any action taken to obtain information by means of a CHIS including any action taken to induce, request of assist a person to act as a CHIS(i.e. What they are asked to do).

#### **Residential Premises**

Means any premises occupied by any person, however temporarily, for residential purposes or otherwise as living accommodation (including hotel or prison accommodation), but does not include common areas to such premises.

#### Premises

This can also include any vehicle or moveable structure used within the definition above.

#### Private Vehicle

Means any vehicle which is used primarily for private purposes of the person who owns it, or otherwise has a right to use it, but would not include any person whose right to use the vehicle arises from making payment for a particular journey.

#### Vehicle

Can also include any vessel, aircraft or hovercraft.

# **Requesting Officer**

This refers to the officer seeking the authorisation

#### D. GENERAL INFORMATION ON RIPA

- 7. The Human Rights Act 1998 (HRA), which brought much of the European Convention on Human Rights and Fundamental Freedom 1950 into UK domestic law, requires the Council (as well as individuals and organisations working on its behalf) to respect the private and family life of citizens, their homes and their correspondence.
- 8. The European Convention did not, however, make this an absolute right but a Qualified Right. Accordingly, in certain circumstances, the Council may interfere in the citizen's rights mentioned above, if such interference is:
- (a) in accordance with the law
- (b) necessary (as defined in this document)
- (c) proportionate (as defined in this document)
- 9. RIPA provides a statutory mechanism (i.e., in accordance with the law) for authorising the use of communications data, covert surveillance and the use and conduct of a CHIS. It seeks to ensure that any interference with the individual's right under Article 8 of the European Convention is necessary and proportionate. In doing

so, RIPA seeks to ensure both the public interest and the human rights of individuals are suitably balanced.

# Does RIPA and this Policy apply to me?

- 10. If an officer undertakes any form of surveillance of individuals or organisations in the conduct of their duties (e.g., as part of the investigatory, enforcement or regulatory functions of the Council), the likely answer is "yes".
- 11Directed surveillance may now only be undertaken in the investigation of criminal offences attracting a penalty of not less than 6 months imprisonment or offences of selling tobacco or alcohol to children. This means that other offences and incidents of disorder may no longer be investigated using covert surveillance.
- 12. If in doubt, staff are required to consult with either the Legal Department or Monitoring Officer rather than open the Council and themselves to the consequences of noncompliance.

# E. THE SCOPE OF RIPA

#### 13. RIPA does:

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

# 14. RIPA does not:

- make unlawful conduct which is otherwise lawful
- Prejudice any existing powers available to the Council to obtain information by any means not involving conduct requiring authorisation under RIPA.

15. For example, it does not affect the Council's current powers to obtain information via the DVLA as to the ownership of vehicles or from the Land Registry as to the ownership of property

#### F. PRINCIPLES OF RIPA - NECESSARY & PROPORTIONATE

## **Necessary**

• 16. For interference with an individuals' rights under Article 8 of the ECHR to be necessary both the Covert Surveillance/use of CHIS MUST bebe for the purpose of preventing or detecting crime or preventing disorder and Directed Surveillance must be for the purpose of investigating a crime attracting a penalty of not less than 6 months imprisonment or a crime relating to the sale of alcohol ot tobacco to children. It is important that officers address the question why surveillance is necessary in this particular case, in that the desired information cannot be reasonably acquired by overt means.

#### **Proportionate**

- 17. Even if the proposed activity is considered to be necessary, the person considering the application for authorisation must consider whether the activities are proportionate to the offence which is being investigated. This involves balancing the intrusiveness of the activity on the target and others who might be affected by it against the need for the activity in operational terms. This element is designed to ensure that the proposed course of action does not represent a sledge hammer being used to crack a walnut. The activity will not be proportionate if:
- The intrusiveness is excessive in relation to the value of the information to be obtained or in relation to the harm being caused by the offence, or
- The information sought could be obtained by less intrusive means.

The least intrusive method is more likely to be considered proportionate by the Courts

#### G. COLLATERAL INTRUSION

- 18. The officer seeking the authorisation should also consider the possibility of COLLATERAL INTRUSION. This is where interference with the privacy of others not subject to the original surveillance may occur. Steps should be taken to assess the risk and, where possible, reduce the risk of collateral intrusion. If there is serious risk of collateral intrusion the proposed surveillance operation would have to be reconsidered and other ways of obtaining the information used if possible. Where unforeseen collateral intrusion occurs during an operation the Authorising Officer must be notified and consideration given to amending the authorisation following a review. Measures must be taken whenever practicable to avoid or minimise so far as is possible any Collateral Intrusion. The risk of this is something which must be considered when determining proportionality.
- 19. Consideration must also be given as to whether or not the surveillance activities of the Service should take place where similar activities are also being undertaken by another agency e.g. the Police, Benefits Agency, Environment Agency.

#### H. SURVEILLANCE

# **Types of Surveillance Examples**

#### 20. Overt

- police officer or parks warden on patrol
- signposted Town Centre CCTV cameras (in normal use)
- recording noise coming from premises outside the premises after the occupier has

been warned that this will occur if the noise persists

 most test purchases (where the officer behaves no differently from a normal member of the public)

# 21. Covert (but not requiring prior RIPA authorisation)

• CCTV cameras providing general traffic, crime or public safety information

# 22. Directed - must be RIPA authorised

- Officers follow an individual or individuals over a period of time to establish whether s/he is working when claiming benefit and committing benefit fraud
- Test purchases where the officer has a hidden camera or other recording device to record information about the private life of a shop owner, e.g., where s/he is suspected of selling alcohol or tobacco to children.
- Officers following an employee to establish whether they are working when off
  on long term sick is directed surveillance which can no longer be undertaken
  in relation to internal disciplinary matters and could only be undertaken if the
  employer is investigating an offence of e:g theft or fraud with the intention of
  prosecuting the individual.

#### 23. Intrusive – must not be undertaken

 Planting a listening or other device (bug) in a person's home or in their private vehicle

24. 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 authorised surveillance
- Surveillance by, or with, the assistance of appropriate surveillance device(s)

Surveillance can be overt or covert.

#### 25. 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 carried out by Environmental Health for food hygiene or other purposes) and/or will be going about Council business openly (e.g., a car parks inspector walking through a car park).

Similarly, surveillance will be overt if the subject has been told that it will happen, e.g. 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.

# 26. Covert Surveillance

Covert surveillance is carried out in a manner calculated to ensure that the person subject to the surveillance is unaware of it taking place. RIPA regulates two types of covert surveillance, namely Directed Surveillance and Intrusive Surveillance as well as the use of CHIS.

#### 27. Directed Surveillance:

- is covert
- is not intrusive surveillance
- is 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) and it 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)

#### 28. Intrusive Surveillance:

- is covert
- relates to residential premises and private vehicles

 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.

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

# I. HANDLING PRODUCTS FROM SURVEILLANCE ACTIVITIES

- 29. Product from Covert Surveillance activities may consist of:
  - Photographs
  - Video film
  - Digital images
  - Voice recordings
  - Surveillance log
  - Officers' Notes
- 30. The above may be required as evidence in current or future criminal proceedings. Officers must have regard to the provisions of the Criminal Procedure and Investigations Act 1996 in relation to unused material. Product obtained via an authorisation may be used by the authority in other investigations but may not be admitted as evidence in relation to offences which do not attract a penalty of at least 6 months imprisonment or relate to the sale of alcohol or tobacco to children.
- 31. Although specific legislation and the Data Protection Act 1998 provide for the disclosure of information in certain circumstances, additional controls are introduced by the Regulation of Investigatory Powers Act.
- 32. The use of any product obtained by authorised surveillance activities outside of the Public Authority or the Courts should only be authorised in the most exceptional circumstances. This requirement seeks to prevent product from being used for grounds other than that for which it was obtained.
- 33. Officers may receive requests from other agencies for product which may include photographs of suspects, descriptions, vehicle details. Where this information has been obtained under an authorisation, further guidance should be sought from the Authorising Officer, since disclosure may not be permitted under the provisions of the Code of Practice

# Storage of Products

34. Officers should ensure that evidential protocols are observed to ensure the integrity, security and confidentiality of material. They will ensure that the requirements of the Seventh Principle of the Data Protection Act are addressed. This principle deals with the security of data.

# **Disposal of Products**

35. Officers should have regard to fifth principle of the Data Protection Act 1998, as follows:

Product which is not required as evidence should not be retained any longer than necessary. It will be necessary to retain product for a sufficient period of time to safeguard Hertsmere Borough Council against any civil claims against infringement of an individual's Human Rights. A PERIOD OF FIVE YEARS ensures that all of the retention period requirements are addressed.

- 36. Product which has been destroyed should have this fact recorded on the record of product obtained by Directed Surveillance, and be signed by the officer.
- 37. An amended copy of this Record form should be forwarded to the Authorising Officer, indicating destruction of the product obtained from the surveillance activity.
- 38. Relevant directorates must ensure that any data is processed in accordance with Data Protection legislation.
- 39. In the case of use of CHIS's, records should be maintained in such a way as to preserve the confidentiality of the source and the information provided by the source.

# J. CONDUCT AND USE OF A COVERT HUMAN INTELLIGENCE SOURCE (CHIS)

- 40. A CHIS is someone who establishes or maintains a personal or other relationship for the covert purpose of helping to obtain information.
- 41. In a local authority, a CHIS is restricted to an informant or an officer working under cover.
- 42. RIPA does not apply in circumstances where members of the public volunteer information to the Council as part of their normal civic duties or to contact numbers set up to receive information.
- 43. The conduct or use of a CHIS requires PRIOR authorisation.

#### 44. A CHIS would not be:

• A member of the public who volunteers information to the local authority, such as a person who complains that they purchased food passed its use by date from their local supermarket. In that case the relationship between customer and provider is too remote. However, if the information were to be provided by an employee of the supermarket who was alleging that the food was being sold past its use by date and who continued to pass information to the Authority while being employed, such a person would be a CHIS i.e. a relationship exists namely one of employer/employee.

- An officer who merely goes into a shop and purchases an item without engaging in dialogue except for "how much"? and "thank you", would not be a CHIS as, although the officer is working under cover, the officer is not seeking information from that person or to gain that person's trust.
- An officer who attends premises and identifies him/herself and then either carries out a statutory inspection or has entered in pursuance of a warrant of entry issued by a court, is not a CHIS. There is nothing covert about their visit.

45. An Authorising Officer should not grant an authorisation for use of a CHIS unless they are satisfied of the following:

- That at all times there will be an officer who will have day to day responsibility for dealing with the source on behalf of the Council and for the source's security and welfare.
- That at all times there will be another officer (senior to the officer having responsibility under bullet point 1 above) who will have general oversight of the use made of the source.
- That at all times there will be an officer responsible for maintaining a record of the use made of the source, and
- That records maintained by the Council, which disclose the identity of the source, will not be available to any personxcept to the extent that there is a need for access to them to be made available to that person.

# 46. How is an Application for a CHIS authorisation made?

An application for authorisation for a Covert Human Intelligence Source (CHIS) must be made in writing. It will specify:

- The reasons why the authorisation is necessary in the particular case and the grounds listed in the Act;
- The reasons why the authorisation is considered proportionate to what it seeks to achieve;
- The purpose for which the source will be tasked or deployed;
- Where a specific investigation or operation is involved, the nature of that investigation or operation;
- Where an authorisation is issued that authorisation will need to be the subject of an application to a Justice of the Peace for judicial approval before it can be acted upon

# 47. Safety and Welfare of a CHIS

The safety and welfare of the source and foreseeable consequences to others should be taken into account in deciding whether or not to grant an authorisation. A risk assessment determining the risk to the source in acting as a source of information to the Council and in particular, identifying and assessing the risks should the identity of the source become known, should be carried out. The welfare and security of the source after operations have ceased should be considered at the outset. The officer having responsibility under Paragraph 8.1 above (i.e. the officer with day to day responsibility for the source) should report to the officer having

general oversight any concerns about the personal circumstances of the source, insofar as they might affect:

- The validity of the risk assessment
- · The conduct of the source, and
- The safety and welfare of the source

The officer having responsibility under paragraph 45 can also be a CHIS and their health and safety should not be overlooked. If officers are to be used as a CHIS, the arrangements mentioned above should be followed so that the source is correctly managed.

#### 48. Juvenile Sources

Special safeguards apply to the use or conduct of Juvenile sources (i.e. under 18 years old). Authorising Officers should abide by The Home Office Code of Conduct relating to Juveniles. Only the Chief Executive may authorise the use of a Juvenile Source

#### 49. Vulnerable Individuals

A vulnerable individual is a person who is or may be in need of community care services by reason of mental or other disability, age or illness, and who is or maybe unable to take care of himself or herself, or unable to protect himself or herself against significant harm or exploitation. Only the Chief Executive may authorise the use of a vulnerable individual as a source.

# 50. Anti-social behaviour activities (e.g. noise, violence, race etc)

Persons who complain about anti-social behaviour, and are asked to keep a diary, will not normally be a CHIS as they are not required to establish or maintain a relationship for a covert purpose. Recording the level of noise (e.g. the decibel level) will not normally capture private information and, therefore, does not require authorisation.

Recording sound (with a DAT recorder) on private premises could constitute Intrusive Surveillance, unless it is done overtly. For example, it will be possible to record if the noisemaker is warned that this will occur if the level of noise continues. Placing a stationary or mobile video camera outside a building to record anti-social behaviour on residential estates is directed surveillance which can no longer be authorised. Such cameras could only be used where notice of such use has been given.

# J. COMMUNICATIONS DATA

In appropriate circumstances an Authorising Officer may authorise the obtaining of Communications Data consisting of service use data or subscriber information but not traffic data.

Where the obtaining of such information is authorised a request is made to the Single Point of Contact (SPoC) provided by the National Anti Frad Network. The application will be approved by the SPoC and returned to

the Authority for the Authority to apply to the Magistrates Court for Judicial Approval. Once this has been obtained it will be returned to the SPoC who will contact the communications service provider to obtain the communications data.

# K. AUTHORISATION PROCEDURES

## **Authorising Officers**

51. The power to grant, renew, review, cancel and reject authorisations will be limited to only those grades of officers detailed below in order to ensure maximum independence and consistency:

A Chief Executive

B Directors of Resources and Environment

C Heads of Service

See Appendix A for the list of officers to whom this applies. This list is updated annually.

- 52. The Monitoring Officer, in conjunction with the Director of Resources, will maintain the above list of Authorising Officers and (as stated in Para 52 above).
- 53. Authorising Officers must not be responsible for authorising investigations/ operations in which they are directly involved although it is recognised that, on occasions, this may be unavoidable. If they do so, this must be declared on the authorising form and noted in the central register.
- 54. Authorising Officers will receive on-going training in RIPA and HRA.
- 55. Urgent Authorisation / Unforeseen Circumstances

It is no longer possible to give Oral Authorisation and all Authorisations need to be in writing and approved by a Justice of the Peace.

# **56. Duration of Authorisations**

The Form must be reviewed in the time stated and cancelled once it is no longer needed.

The Authorisation to carry out/conduct surveillance will expire as follows:

- Directed Covert Surveillance 3 months (from date of authorisation)
- CHIS 12 months (from date of authorisation)

# L. INFORMATION FOR APPLICANTS/REQUESTING OFFICERS

- 57. The application should include:
  - The grounds on which the authorisation is sought.

- The reasons why the authorisation is necessary in the particular case and on the ground i.e. See paragraph; 9.4 for the purpose of preventing or detecting crime or for preventing disorder.
- The reasons why the surveillance is considered proportionate to what it seeks to achieve:
- The action to be authorised;
- The nature of the surveillance;
- · An account of the investigation or operation;
- 58. The identities, where know, of those to be the subject of the surveillance; an explanation of the information which it is desired to obtain as a result of the surveillance:
  - The details of any potential collateral intrusion and why the intrusion is justified;
  - The details of any confidential information that is likely to be obtained as a consequence of the surveillance.
  - The level of authority required (or recommended where that is different) for the surveillance; and
  - A subsequent record of whether authority was given or refused, by whom and the time and date.

# Procedure for obtaining Judicial Approval

An application form will need to be submitted to the Magistrates Court with a copy of the Authorisation and the supporting documents setting out the case.

The Court will arrange a hearing before a single Justice of the Peace. No notice of the hearing will need to be given to the subject of the proposed surveillance but an appropriate officer will need attend the hearing to make the application for Judicial Approval. Since the hearing is a legal proceedings the officer representing the Council will need to be duly authorised unless legally qualified to appear.

The original Authorisation will need to be produced and the officer will need to have prepared a draft judicial application form/order for completion by the JP.

The procedure will be the same for the obtaining of Judicial Approval of a Renewal of an Authorisation.

# N. RECORDS MANAGEMENT

- 60. The Council must keep a detailed record of all authorisations, renewals, cancellations and rejections in Service Areas and provide a copy to the Director of Resources A Central Register of all authorisations, renewals, cancellations and rejections will be maintained by the Monitoring Officer in conjunction with the Director of Resources.
- 61. The following documents must be retained:
  - A copy of the forms together with any supplementary documentation and notification of the approval given by the Authorising Officer

- A copy of the Judicial Approval Order
- 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, together with the supporting documentation submitted when the renewal was requested
- A copy of the Judicial Approval Order for any Renewal
- The date and time when any instruction was given by the Authorising Officer
- The Unique reference Number for the authorisation (URN)

62. The Council will retain records for a period of at least three years from the ending of an authorisation. This will facilitate any inspection undertaken by the Office of Surveillance Commissioners.

# Appendix - Names of Authorising Officers

Position/Grade	Name of Authorising Officer
Chief Executive	Donald Graham
Director of Resources	Sajida Bijle
Director of Environment	Glen Wooldrige
Head of Corporate Support	Hilary Shade
Head of Financial and Business Services	Dev Gopal
Head of Human Resources and	Judith Fear
Customer Services	
Head of Waste and Street Scene	Steve Burton