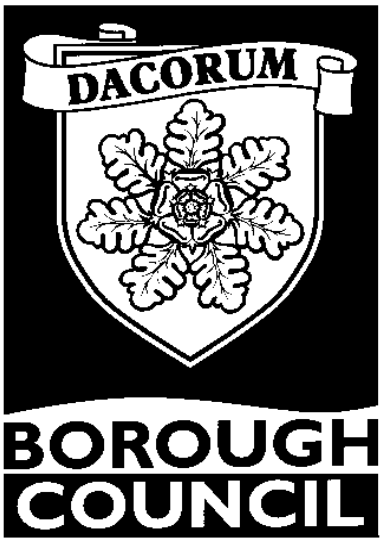

CORPORATE POLICY & PROCEDURES DOCUMENT FOR COVERT SURVEILLANCE AND THE USE OF COVERT HUMAN INTELLIGENCE SOURCES

PREPARED IN COMPLIANCE WITH THE REGULATION OF INVESTIGATORY POWERS ACT 2000 AND THE REVISED HOME OFFICE CODES OF PRACTICE ISSUED IN AUGUST 2018

AUTHOR: MARK BROOKES, ASSISTANT DIRECTOR (LEGAL AND DEMOCRATIC SERVICES), EXT 2236

FIRST PUBLISHED: 2005

LAST REVIEWED: February 2024

CONTENTS PAGE

NB:
The Regulation of Investigatory Powers Act 2000 ('RIPA') refers to 'Designated Officers'. For ease of understanding and application within Dacorum Borough Council, this Corporate Policy & Procedures Document refers to 'Authorising Officers'. Furthermore, such Officers can only act under RIPA if they have been duly certified by the Council's Assistant Director (Legal and Democratic Services). For the avoidance of doubt, therefore, all references to duly certified Authorising Officers refer to 'Designated Officers' under RIPA.

.

A. Introduction and Key Messages

1. This Corporate Policy & Procedures Document is based upon the requirements of Part II of Regulation of Investigatory Powers Act 2000 ('RIPA'), the Investigatory Powers Act 2016 and the revised Codes of Practice issued by the Home Office pursuant to Section 71 of RIPA(August 2018). The authoritative position on RIPA is, of course, the Act itself and the Home Office's Codes of Practice on Covert Surveillance and Covert Human Intelligence Sources. Any officer who is unsure about any aspect of this document should contact, at the earliest possible opportunity, the Council's Assistant Director (Legal and Democratic Services), for advice and assistance. The revised Codes of Practice can be downloaded from the Home Office web site or a hard copy can be obtained from the Assistant Director (Legal and Democratic Services).

2. This document and the related forms can be found on the Council's Intranet.

3. The Assistant Director (Legal and Democratic Services) will maintain and check the Corporate Register of all RIPA authorisations, reviews, renewals, cancellations and rejections. It is the responsibility of the relevant Authorising Officer, however, to ensure the Assistant Director (Legal and Democratic Services) receives a copy of the relevant forms within 1 week of authorisation, review, renewal, cancellation or rejection.

4. RIPA, the Codes of Practice and this document are important for the effective and efficient operation of the Council's actions with regard to covert surveillance and Covert Human Intelligence Sources. This document will, therefore, be kept under review by the Assistant Director (Legal and Democratic Services). Authorising Officers must bring any suggestions for continuous improvement of this document to the attention of the Assistant Director (Legal and Democratic Services) at the earliest possible opportunity.

5. If you are in any doubt on RIPA, the Codes of Practice, this document or the related legislative provisions, please consult the Assistant Director (Legal and Democratic Services).

B. Borough Council Policy Statement

1. The Council takes seriously its statutory responsibilities and will, at all times, act in accordance with the law, and take necessary and proportionate action in these types of enforcement matters involving the use of covert surveillance. In that regard, the Assistant Director (Legal and Democratic Services), is duly authorised by the Council's Corporate Management Team as the Council's 'Senior Responsible Officer' with responsibility to keep this document up to date and to amend, delete, add or substitute relevant provisions, as necessary. For administration and operational effectiveness, the Assistant Director (Legal and Democratic Services) is also authorised to add or substitute officers authorised for the purpose of RIPA.

,

C. General Information on RIPA

1. The Human Rights Act 1998 (which incorporated the European Convention on Human Rights into UK law) requires the Council, and organisations working on its behalf, to respect the private and family life of the citizen, his/her home and his/her correspondence.

2. This is not an absolute right, but a qualified right. Accordingly, in certain circumstances, the Council, as a 'Relevant Public Authority' under RIPA, may interfere in the citizen's right to privacy mentioned above, if such interference is: -

   (a) **in accordance with the law;**

   (a) **necessary** (as defined in this document); **and**

   (b) **proportionate** (as defined in this document).

3. RIPA provides a statutory mechanism for authorising **directed surveillance** and the use of a **'covert human intelligence source' ('CHIS').** Directed surveillance is defined later in section E, but is essentially surveillance which is covert and is carried out in places other than residential premises or private vehicles. A CHIS is a person used by the Council to establish or maintain a personal or other relationship with another person for the covert purpose of obtaining information (e.g. undercover agents). RIPA seeks to ensure that any interference with an individual's right under the Human Rights Act 1998 is **necessary** and **proportionate**. In doing so, RIPA seeks to ensure both the public interest and the human rights of individuals are suitably balanced.

4. Directed surveillance can only be authorised under RIPA to prevent or detect criminal offences that are either punishable, whether on summary conviction or indictment, by a maximum term of at least 6 months imprisonment or are related to the underage sale of alcohol and tobacco. The offences relating to the latter are set out in section E. This crime threshold applies only to the authorisation of directed surveillance under RIPA, not to the authorisation of the use of CHIS.

5. An authorisation for the use of directed surveillance or the use of a CHIS can only take effect once an order approving the authorisation has been granted by a Justice of the Peace (JP). This also applies to a **renewal** of an authorisation.

6. Directly employed Council staff and external agencies working for the Council are covered by RIPA for the time they are working for the Council. All external agencies must, therefore, comply with RIPA and the work carried out by agencies on the Council's behalf must be properly authorised by one of the Council's designated Authorising Officers. Authorising Officers are those whose posts appear in **Appendix 1** to this document and, duly added to or substituted by the Assistant Director (Legal and Democratic Services).

7. If the correct RIPA procedures are not followed, evidence may be disallowed by the courts, a complaint of maladministration could be made to the Ombudsman, and/or the Council could be ordered to pay compensation. Such action would, of course, harm the reputation of the Council and will, undoubtedly, be the subject of adverse press and media interest. It is essential, therefore, that all Council staff involved with RIPA comply

with this document and any further guidance that may be issued, from time to time, by the Assistant Director (Legal and Democratic Services).

8. A flowchart of the procedures to be followed appears at **Appendix 2**.

9. **Necessity and proportionality**

9.1 The Authorising Officer must –

- believe that the surveillance activities which are being authorised are **necessary for the purpose of preventing or detecting crime or of preventing disorder** and,

  in the case of **directed surveillance**

- be satisfied that what is being investigated is a criminal offence which meets the threshold.

This is the only statutory ground available for local authorities for the use of covert surveillance. The Authorising Officer must also believe that the surveillance activities are **proportionate** to what is sought to be achieved by carrying them out. This involves balancing the seriousness of the intrusion into the privacy of the person who is the subject of the operation (or any other person who may be affected) against the need for the surveillance in investigative and operational terms.

9.2 The authorisation will not be proportionate if it is excessive in the overall circumstances of the case. Each action authorised should bring an expected benefit to the investigation or operation and should not be disproportionate or arbitrary. The fact that a suspected offence may be serious will not alone render intrusive actions proportionate.

9.3 The following elements of proportionality should therefore be considered:

- Balancing the size and scope of the proposed activity and the potential intrusion into the subject's personal life against the gravity and extent of the perceived crime or offence;

- Explaining how and why the methods to be adopted will cause the least possible intrusion on the subject and others;

- Considering whether the activity is an appropriate use of RIPA and a reasonable way, having considered all reasonable alternatives, of obtaining the necessary result;

- Evidencing, as far as reasonably practicable, what other methods had been considered and why they were not used

10. **Collateral intrusion**

Before authorising applications for directed surveillance, the Authorising Officer should also take into account the risk of obtaining private information about persons who are not the subjects of the surveillance (members of the subject's family for example). This is

referred to as collateral intrusion. All applications should include an assessment of the risk of collateral intrusion and details of any measures taken to limit this. The same proportionality tests apply to the likelihood of collateral intrusion as to intrusion into the privacy of the intended subject of the surveillance. The Authorising Officer must therefore consider fully the proportionality of the proposed actions.

D. What RIPA Does and Does Not Do

1. **RIPA does**:

- require prior authorisation of directed surveillance.
- prohibit the Council from carrying out intrusive surveillance.
- require authorisation of the conduct and use of a CHIS
- require safeguards for the conduct and use of a CHIS
- require judicial approval before authorisations for the use of directed surveillance or the use of CHIS can take effect.

2. **RIPA does not**:

- make conduct unlawful where it would be otherwise lawful.
- prejudice or dis-apply any existing powers available to the Council to obtain information by any means not involving conduct that may be authorised under RIPA. For example, it does not affect the Council's current powers to obtain information via the DVLA or to get information from the Land Registry as to the ownership of a property.

3. If the Authorising Officer or any Applicant is in any doubt, s/he should ask the Assistant Director (Legal and Democratic Services) BEFORE any directed surveillance and/or CHIS is authorised, renewed, cancelled or rejected.

E. Types of Surveillance

1. **'Surveillance'** includes

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

Surveillance can be overt or covert.

2. **Overt Surveillance**

Most of the surveillance carried out by the Council will be done overtly – there will be nothing secretive, clandestine or hidden about it. In many cases, Officers will be behaving in the same way as a normal member of the public (e.g. in the case of most test purchases), and/or will be going about Council business openly (e.g. a market inspector walking through markets).

3. Similarly, surveillance will be overt if the subject has been told it will happen (e.g. where a noisemaker is warned (preferably in writing) 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 identifying themselves to the owner/proprietor to check that the conditions are being met.

4. **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. (Section 26(9)(a) of RIPA).

5. RIPA regulates two types of covert surveillance: directed surveillance and intrusive surveillance and the use of Covert Human Intelligence Sources (CHIS).

6. **Directed Surveillance**

6.1 Directed Surveillance is surveillance which: -

- is covert; and
- is not intrusive surveillance (see definition below – the Council must not carry out any intrusive surveillance);
- is not carried out in an immediate response to events which would otherwise make seeking authorisation under RIPA 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). (*Section 26(10) of RIPA).*

6.2 Directed Surveillance Crime Threshold

The use of directed surveillance can only be authorised under RIPA to prevent or detect criminal offences that are punishable, whether on summary conviction or indictment, by a maximum term of at least 6 months imprisonment or are related to the underage sale of alcohol and tobacco. The offences relating to the latter are sections 146, 147 and 147A of the Licensing Act 2003 and section 7 of the Children and Young Persons Act 1933. This means that-

- directed surveillance cannot be authorised for the purpose of preventing disorder unless this involves a criminal offence punishable by at least 6 months imprisonment

- directed surveillance can be authorised for the purpose of preventing or detecting specified criminal offences relating to the underage sale of alcohol and tobacco where the necessity and proportionality tests are met and prior approval from a JP has been granted.

7. **Private information**

In relation to a person 'private information' includes any information relating to his private and family life, his home and his correspondence. It should be taken generally to include any aspect of a person's private or personal relationship with others, including family and professional or business relationships. 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. This is likely to be the case where that person has a reasonable expectation of privacy even though acting in public and where the Council is making a record of that person's activities for future consideration or analysis.

Example: Two people holding a conversation in a street, or on a bus, may have a reasonable expectation of privacy over the contents of their conversation, even though they are associating in public. The contents of such a conversation should still be considered as private information.

Private life considerations are particularly likely to arise if several records are to be analysed together in order to establish, for example, a pattern of behavior.

Example: Council officers wish to drive past a café for the purposes of obtaining a photograph of the exterior. Reconnaissance of this nature is not likely to require a directed surveillance authorisation as no private information about any person is likely to be obtained or recorded. However, if the Council wished to repeat the exercise, for example to establish a pattern of occupancy of the premises by any person, the accumulation of information is likely to result in the obtaining of private information about that person and a directed surveillance authorisation would be required.

Prolonged surveillance targeted on a single person will undoubtedly result in the obtaining of private information about him/her and others that s/he comes into contact, or associates, with.

8. Similarly, although overt town centre CCTV cameras do not normally require authorisation, if a particular camera is being used for a specific purpose, which involves prolonged surveillance on a particular person, authorisation will be required. The way a

person runs his/her business may also reveal information about his or her private life and the private lives of others.

9. **Confidential information**

Special consideration must be given to authorisations that involve confidential personal information. Where such material has been acquired and retained, the matter should be reported to the Assistant Director (Legal and Democratic Services) so that s/he can inform the Office of Surveillance Commissioners or Inspector during his next inspection and the material made available to him if requested.

Confidential personal information is information held in confidence relating to the physical or mental health or spiritual counselling of a person (whether living or dead) who can be identified from it. Such information, which can include both oral and written communications, 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.

Examples include consultations between a health professional and a patient, or information from a patient's medical records.

10. For the avoidance of doubt, only those Officers designated and certified to be 'Authorising Officers' for the purpose of RIPA can authorise 'Directed Surveillance' if, and only if, the RIPA authorisation procedures detailed in this document are followed. If an Authorising Officer has not been 'certified' for the purposes of RIPA, s/he can not carry out or approve/reject any action set out in this Corporate Policy & Procedures Document.

Only the Chief Executive can authorise applications for covert surveillance when knowledge of confidential information is likely to be acquired.

11. **Intrusive Surveillance**

This is when it: -

- is covert;
- relates to anything taking place on residential premises or in any private vehicle;
- 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 includes any part of premises which are being occupied or used by any person, however temporarily, for residential purposes or otherwise as living accommodation. It includes hotel accommodation. However, common areas to which a person has access in connection with their use or occupation of accommodation are excluded from the definition of residential premises.

Examples of common areas of residential premises which are excluded would include:

- a communal stairway in a block of flats;
- a hotel reception area or dining room;
- the front garden or driveway of premises readily visible to the public.

A private vehicle is any vehicle which is used primarily for the private purposes of the person who owns it or a person otherwise having the right to use it. This includes, for example, a company car, owned by a leasing company and used for business and pleasure by the employee of a company.

Local authorities are not allowed to carry out intrusive surveillance and therefore no Council officer can authorise a covert surveillance operation if it involves intrusive surveillance as defined above.

12. **Where authorisation is not required**

Some surveillance activity does not constitute directed surveillance under RIPA and therefore authorisations are not required. Such activity includes:

- covert surveillance by way of an immediate response to events;
- covert surveillance as part of general observation activities;
- covert surveillance not relating to the prevention or detection of crime or the prevention of disorder;
- overt use of CCTV
- specific situations not requiring an authorization

These types of surveillance activity are explained in more detail below.

13. **Immediate response**

Covert surveillance that is likely to reveal private information about a person but is carried out by way of an immediate response to events such that it is not reasonably practicable to obtain an authorisation under RIPA.

Example: An authorisation would not be required where Council officers conceal themselves in order to observe an incident that they happen to come across where a person appears to be in the act of illegally dumping waste.

14. **General observation activities**

The general observation duties of many Council enforcement officers do not require authorisations under RIPA.

Example: Public protection officers attending an anti-social behaviour hot-spot would not normally require an authorisation provided their objective was to merely observe the location to ascertain the extent of the problem and to see whether individuals can be identified. The activity may be part of a specific investigation but is general observational activity, rather than targeted surveillance of individuals, and the obtaining of private information is unlikely.

15. **Not related to the prevention or detection of crime or the prevention of disorder**

In the case of local authorities directed surveillance can only be authorised under RIPA if it is for the purpose of preventing or detecting crime or of preventing disorder. Covert surveillance for any other general purposes should be conducted under other relevant legislation. A local authority can only use RIPA in relation to its 'core functions' i.e, the 'specific public functions' undertaken by a particular authority in contrast to the 'ordinary functions' undertaken by all authorities (e.g. employment issues).

Example: A Council employee is off work due, he claims, to an injury sustained at work for which he is suing the Council. The employee's manager suspects the employee is exaggerating the seriousness of their injury and that they are, in fact, fit enough to come to work. The manager wishes to place the employee under covert surveillance outside of his normal work environment to establish that he is indeed fit for work and to gather evidence for disciplinary proceedings against the employee for deceiving the Council. Such surveillance, even though likely to result in obtaining private information, does not constitute directed surveillance under RIPA as it does not relate to the Council's core functions. It relates instead to the carrying out of its employment functions which are common to all authorities. Surveillance of this nature would be covered by the Data Protection Act 1998 and the Council's own employment policies.

16. **CCTV**

The use of overt CCTV cameras does not normally require an authorisation under RIPA. Their operation is covered by the Data Protection Act 1998 and the code of practice issued by the Information Commissioner's Office in October 2014 entitled 'In the picture: A data protection code of practice for surveillance cameras and personal information'.

However, where overt CCTV cameras are used in a covert and pre-planned manner as part of a specific investigation or operation, for the targeted surveillance of a specific person or group of people, an authorisation will be required.

17. **Specific situations not requiring an authorisation**

There are a number of specific situations which do not require an authorisation under RIPA. The specific situations most relevant to the Council are –

- the overt or covert recording of an interview of a member of the public where it is made clear that the interview is entirely voluntary and that the interviewer is a Council officer;

- the covert recording of suspected noise nuisance where the intention is only to record excessive noise levels from adjoining premises and the recording device is calibrated to record only excessive noise levels.

18. ***Examples of different types of Surveillance***

Type of Surveillance	Examples
Overt	- Police Officer or Estates Warden on patrol - Signposted Town Centre CCTV cameras (in normal use) - Recording noise coming from 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).
Covert but not requiring prior authorisation	- CCTV cameras providing general traffic, crime or public safety information
Directed must be RIPA authorised.	- Officers follow an individual or individuals over a period, to establish whether s/he is working when claiming benefit or off long term sick from employment. - Test purchases where the officer has a hidden camera or other recording device to record information which might include information about the private life of a shop-owner, e.g. where s/he is suspected of running his business in an unlawful manner.
Intrusive – **Council cannot do this!**	- Planting a listening or other device (bug) in a person's home or in their private vehicle.

F. Conduct and Use of a Covert Human Intelligence Source (CHIS)

Who is a CHIS?

1. Someone who establishes or maintains a personal or other relationship for the covert purpose of helping the covert use of the relationship to obtain information. **In normal circumstances the Council will not use a CHIS. If consideration is given to the use of a CHIS the Assistant Director (Legal and Democratic Services) must be consulted first.**

2. RIPA does not normally 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.

What must be authorised?

3. The conduct or use of a CHIS requires prior authorisation.

   - **Conduct** of a CHIS = Establishing or maintaining a personal or other relationship with a person for the covert purpose of (or is incidental to) obtaining and passing on information.

   - **Use** of a CHIS = Actions inducing, asking or assisting a person to act as a CHIS and the decision to use a CHIS in the first place.

4. **If a CHIS is used the RIPA procedures, detailed in this document, must be followed. As with directed surveillance, authorisations for the use of a CHIS cannot take effect until an order has been obtained from a JP. However, the crime threshold which applies to directed surveillance does not apply to the use of a CHIS.**

Juvenile Sources

5. Special safeguards apply to the use or conduct of juvenile sources (i.e. under 18 year olds). On no occasion can a child under 16 years of age be authorised to give information against his or her parents.

   Authorisations for juvenile sources shall also not be granted unless special provisions contained within the Regulation of Investigatory Powers (Juveniles) Order 2000 (as amended), are satisfied. The duration of such an authorisation is **four months** from the time of grant or renewal (instead of twelve months), and the authorisation should be subject to at least monthly review.

   Only the Chief Executive or, in his or her absence, the person deputising for him or her can authorise the use of Juvenile Sources.

   See paragraph 4.2 of the Home Office guidance “Covert Human Intelligence Sources” 2018 for further guidance.

Vulnerable Individuals

6. A 'vulnerable individual' is a person who is or may be in need of community care services by reason of a mental or physical disability, age or illness, and who is or may be unable to take care of himself or herself, or unable to protect himself or herself against significant harm or exploitation.

7. A vulnerable individual will only be authorised to act as a source in the most exceptional of circumstances.

Only the Chief Executive or, in his or her absence, the person deputising for him or her can authorise the use of vulnerable individuals.Test Purchases

9. Carrying out test purchases will not (as highlighted above) require the purchaser to **establish a relationship with the supplier with the covert purpose of obtaining information** and, therefore, the purchaser will not normally be a CHIS.

For example, authorisation would not normally be required for test purchases carried out in the ordinary course of business (e.g. walking into a shop and purchasing a product over the counter).

10. By contrast, "entrapment cases" could require a prior CHIS authorisation if the foregoing criteria were present.

For example, Licensing Officers who pretend to be fares to catch unwary private hire vehicles doing unlicensed pick-ups.

Developing a relationship with a person in the shop, to obtain information about the seller's suppliers of an illegal product (e.g. illegally imported products) will require authorisation as a CHIS.

Similarly, using mobile hidden recording devices or CCTV cameras to record what is going on in the shop will require authorisation as directed surveillance.

A combined authorisation can be given for a CHIS and also directed surveillance.

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

10. 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.

11. 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 (preferably in writing) 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 will require prior authorisation.

G. Authorising Officer Responsibilities

1. The Assistant Director (Legal and Democratic Services) will ensure that sufficient numbers of Authorising Officers are duly certified to take action under this document.

2. It will be the responsibility of Authorising Officers who have been duly certified to ensure their relevant members of staff are suitably trained as 'Applicants' so as to avoid common mistakes appearing on forms for RIPA authorisations.

3. Authorising Officers will also ensure that staff who report to them follow this Corporate Policy & Procedures Document and that they do not undertake or carry out any form of surveillance without first complying with the requirements of this document.

4. Authorising Officers must also pay particular attention to any health and safety issues that may be raised by any proposed surveillance activity. Under no circumstances, should an Authorising Officer approve any RIPA form unless, and until s/he is satisfied that a proper risk assessment has been carried out and the health and safety of Council employees/agents are suitably addressed and/or risks minimised, so far as is possible. If an Authorising Officer is in any doubt, s/he should obtain prior guidance on the same from his/her manager, the Council's Corporate Health & Safety Lead Officer or the Assistant Director (Legal and Democratic Services).

5. Authorising Officers must also ensure that, when sending copies of any forms to the Assistant Director (Legal and Democratic Services) (or any other relevant authority), the same are sent in **sealed** envelopes and marked '**Strictly Private & Confidential'**.

H. Authorisation Procedures

1. Directed surveillance and the use of a CHIS can only be lawfully carried out if properly authorised, and in strict accordance with the terms of the authorisation. **Appendix 2** provides a flow chart of the process from application to recording of information.

Authorising Officers

2. Forms can only be signed by officers of the Council who are at the level of Chief Officer, Assistant Director, or Head of Service and are named as Authorising Officer in **Appendix 1** .

   Only the Chief Executive or, in his or her absence, the person deputising for him or her can authorise an application for directed surveillance when confidential information is likely to be acquired.

   This Appendix will be kept up to date by the Assistant Director (Legal and Democratic Services), and added to as needs require. If a Chief Officer wishes to add, delete or substitute a post, s/he must refer such request to the Assistant Director (Legal and Democratic Services) for consideration, as necessary. The Assistant Director (Legal and Democratic Services) is authorised to add, delete or substitute posts listed in **Appendix 1**.

3. Authorisations under RIPA are separate from delegated authority to act under the Council's Constitution. RIPA authorisations are for specific investigations only, and must be renewed or cancelled once the specific surveillance is complete or about to expire. **The authorisations do not lapse with time!**

4. If the Assistant Director (Legal and Democratic Services) feels that an Authorising Officer has not complied fully with the requirements of this document, he/she may retract that Officer's authorisation until s/he has undertaken appropriate training or a one-to-one meeting with him/her.

Application Forms

5. Only the approved RIPA forms set out in this document must be used. Any other forms will be rejected by the Authorising Officer and/or the Assistant Director (Legal and Democratic Services).

6. **Directed Surveillance and use of Covert Human Intelligence forms – See Appendix 3**

   Form RIP 1 **Application** for Authority for Directed Surveillance
   Form RIP 2 **Renewal** of Directed Surveillance Authority
   Form RIP 3 **Cancellation** of Directed Surveillance
   Form RIP 4 **Review** of Directed Surveillance
   Form RIP 5 **Application** for use of Covert Human Intelligence Source
   Form RIP 6 **Renewal** of authorisation for use of Covert Human Intelligence Source
   Form RIP 7 **Cancellation** of Covert Human Intelligence Source
   Form RIP 8 **Review** of use of Covert Human Intelligence Source

Grounds for Authorisation

7. Directed Surveillance (form RIP 1) and the use of a CHIS (Form RIP 5) can only be authorised by the Council for the **prevention or detection of crime or the prevention of disorder**. As explained in sections C and E above, authorisations for **directed surveillance** are also subject to the crime threshold test.

Assessing the Application Form

8. Before an Authorising Officer signs a Form, **s/he must**: -

(a) Have due regard for RIPA, the Home Office revised Codes of Practice, the Human Rights Act 1998, this Corporate Policy & Procedures Document and any other guidance issued, from time to time, by the Assistant Director (Legal and Democratic Services on such matters;

(b) Satisfy his/herself that the RIPA authorisation is: -

(i) **in accordance with the law**;

(ii) **necessary** in the circumstances of the particular case on the ground mentioned above;

(iii) **proportionate** to what it seeks to achieve;

and in the case of **directed surveillance**,

(iv) be satisfied that what is being investigated is a criminal offence which meets the crime threshold test.

(c) 'Proportionate' means the Authorising Officer must believe that intruding upon someone's privacy through surveillance is proportionate to the desired outcome taking into account the size of the problem as against the breach of privacy

In assessing whether or not the proposed surveillance is proportionate, the Authorising Officer must be satisfied that the application form demonstrates that every other reasonable means of gathering the information has been considered and explains why the alternative means considered would not be likely to achieve the desired outcome. The Authorising Officer must also be satisfied that the proposed method of surveillance is the least intrusive.

The proportionality test is explained in more detail in paragraph 7 above.

The Authorising Officer must in each case follow the "five Ws" (i.e, who, what, where, when and why) incorporated into the forms to make clear what is being authorised. They must also explain how and why they are satisfied that the proposed action is both **necessary** and **proportionate**. It is not enough simply to state that it is so – the reasons **why** it is so must be given.

Every question on the application form must be dealt with fully, following the prompts which are now incorporated in the forms.

(d) Take into account the risk of accidental intrusion into the privacy of persons other then the specified subject of the surveillance (**collateral** intrusion). Measures must be taken wherever practicable to avoid or minimise (so far as is possible) collateral intrusion and the matter may be an aspect of determining proportionality;

(e) Set a date for review of the authorisation and review on only that date;

(f) Allocate a Unique Reference Number (URN) for the application as follows: -.

Year / Service / Number of Application

(g) Ensure that any RIPA Service Register is duly completed, and that a copy of the RIPA Forms (and any review/cancellation of the same) is forwarded to the Assistant Director (Legal and Democratic Services) for inclusion in the Central Register, **within 1 week of the relevant authorisation, review, renewal, cancellation or rejection**.

Additional Safeguards when Authorising a CHIS

9. When authorising the conduct or use of a CHIS, the Authorising Officer **must also: -**

   (a) be satisfied that the **conduct** and/or **use** of the CHIS is proportionate to what is sought to be achieved;

   (b) be satisfied that **appropriate arrangements** are in place for the management and oversight of the CHIS and name the handler and controller in the application (RIPA section 29(5); and this must address health and safety issues through a risk assessment (to be signed off by the Authorising Officer)

   (c) consider the likely degree of intrusion of all those potentially affected;

   (d) consider any adverse impact on community confidence that may result from the use or conduct or the information obtained; and

   (e) ensure **records** containing particulars are not available except on a need to know basis.

Duration

10. The Form **must be reviewed in the time stated (which can be any time stated in the application) and cancelled** once it is no longer needed. The 'authorisation' to carry out/conduct the surveillance lasts for a maximum of 3 months (from authorisation) for directed surveillance and 12 months (from authorisation) for a CHIS (but limited to 4 months for a juvenile source). However, whether the surveillance is carried out/conducted or not, in the relevant period, does not mean the 'authorisation' is 'spent'. In other words, **the Forms do not expire and remain 'live' until cancelled!** The forms must be reviewed and/or cancelled (once they are no longer required)!

11. Authorisations can be renewed in writing at any time before the expiry date, although it is advisable for an application for renewal not to be made until shortly before the expiry date. Authorisations can be renewed more than once if they continue to meet the criteria for authorisations. The Authorising Officer must consider the matter afresh, including taking into account the benefits of the surveillance to date, and any collateral intrusion that has occurred. The Authorising Officer must still be satisfied that the surveillance is still necessary and proportionate.

12. The renewal will begin on the day when the authorisation would have expired.

The Need For Judicial Approval

13. If the Council wishes to authorise the use of directed surveillance or the use of a CHIS under RIPA it will need to obtain an order approving the grant **or renewal** from a **Justice of the Peace** before it can take effect. The JP must be satisfied that the statutory tests have been met and that the use of the covert surveillance is necessary and proportionate before he/she can issue an order approving the use of the covert surveillance described in the application.

14. The judicial approval process is in addition to the authorisation process under the relevant parts of RIPA as outlined in the Codes of Practice. Therefore, the process of assessing necessity and proportionality, completing the RIPA application form and seeking the approval of the Authoring Officer remains the same.

15. When the RIPA application form has been completed and authorised by the Authorising Officer it must be given to the Assistant Director (Legal and Democratic Services) who will arrange for a member of the Council's Legal Team to arrange a hearing date at the magistrates court as early as possible. The member of the Legal Team will complete the judicial application/order form kept by the Assistant Director (Legal and Democratic Services) for the purpose and will attend the hearing with the investigating officer. The original RIPA authorisation will need to be shown to the JP but this will be brought back to the office, together with a copy of the signed order (if granted), and given to the Assistant Director (Legal and Democratic Services) so that it can be placed on the Central Register.

16. As the judicial approval process also applies to applications for the renewal of an authorisation it is important to ensure that the application for judicial approval is made in good time before the deadline for the renewal expires. For example, the renewal deadline may expire when the magistrates court is not sitting (holiday periods for example) in which case the renewal application will need to be brought forward before the holiday period starts.

I. Working With / Through Other Agencies

1. When some other agency has been instructed on behalf of the Council to undertake any action under RIPA, this document and the forms in it must be used as normal and the agency advised or kept informed, as necessary, of the various requirements. They must be made aware explicitly what they are authorised to do.

2. When some other agency (e.g. Police, Customs & Excise, Inland Revenue etc): -

   (a) wish to use the Council's resources (e.g. CCTV surveillance systems), that agency must use its own RIPA procedures and, before any officer agrees to allow the Council's resources to be used for the other agency's purposes, s/he must obtain a copy of that agency's RIPA form for the record (a copy of which must be passed to the Assistant Director (Legal and Democratic Services) for the Central Register) and/or relevant extracts from the same which are sufficient for the purposes of protecting the Council and the use of its resources;

   (b) wish to use the Council's premises for their own RIPA action, the officer should, normally, co-operate with the same, unless there are security or other good operational or managerial reasons as to why the Council's premises should not be used for the agency's activities. Suitable insurance or other appropriate indemnities may be sought, if necessary, from the other agency for the Council's co-operation in the agent's RIPA operation. In such cases, however, the Council's own RIPA forms should not be used as the Council is only 'assisting' and not being 'involved' in the RIPA activity of the external agency.

3. With regards to paragraph 2(a) above, if the Police or other Agency wish to use Council resources for general surveillance, as opposed to specific RIPA operations, an appropriate letter requesting the proposed use, extent of remit, duration, who will be undertaking the general surveillance and the purpose of it must be obtained from the Police or other Agency before any Council resources are made available for the proposed use.

4. **If in doubt, please consult with the** Assistant Director **(**Legal and Democratic Services) **at the earliest opportunity.**

J. Record Management

1. **The Council must keep a detailed record of all authorisations, renewals, cancellations and rejections and a Central Register of all Authorisation Forms will be maintained and monitored by the Assistant Director (**Legal and Democratic Services **).**

2. **Records Maintained**

The following documents must be retained by the Assistant Director (Legal and Democratic Services) (or his/her designated co-ordinator) for such purposes.

- a copy of the Forms together with any supplementary documentation and notification of the approval given by the Authorising Officer;
- a record of the period over which the surveillance has taken place;
- the frequency of reviews prescribed by the Authorising Officer;
- a record of the result of each review of the authorisation;
- a copy of any renewal of an authorisation, together with the supporting documentation submitted when the renewal was requested;
- the date and time when any instruction was given by the Authorising Officer;
- the Unique Reference Number for the authorisation (URN).

3. Each form will have a URN. The service co-ordinators will issue the relevant URN to Applicants. The cross-referencing of each URN takes place within the Forms for inspection purposes. The relevant Service code to be followed is as per **Appendix 1**. Rejected Forms will also have URN's.

Central Register maintained by the Assistant Director (Legal and Democratic Services)

4. Authorising Officers must forward details of each form to the Assistant Director (Legal and Democratic Services for the Central Register, within 1 week of the authorisation, review, renewal, cancellation or rejection. The Assistant Director (Legal and Democratic Services) will monitor the same and give appropriate guidance, from time to time, or amend this document, as necessary.

5. The Council will retain records for a period of at least three years from the ending of the authorisation. The Office of the Surveillance Commissioners (OSC) can inspect the Council's policies and procedures, and individual authorisations.

Retention and Destruction of Evidence

6. Where evidence gathered from surveillance could be relevant to future or pending court proceedings, it should be retained in accordance with established disclosure requirements for a suitable period, commensurate to any subsequent review. Particular attention should be paid to the Criminal Procedure and Investigations Act 1996 which requires evidence gathered in criminal investigations to be recorded and retained.

K. Investigatory Powers Act 2016 - Communications Data

Part 3 of the Investigatory Powers Act 2016 (IPA) replaced Part 1 chapter 2 of RIPA in relation to the acquisition of communications data and puts local authorities on the same standing as the police and law enforcement agencies. Previously the Council had been limited to obtaining subscriber details (known now as 'entity data') such as the registered user of a telephone number or email address. Under the IPA, the Council can now also obtain details of in and out call data and cell site location. This information identifies who a criminal suspect is in communication with and whereabouts the suspect was when they made or received a call, or the location from which they were using an internet service. This additional data is defined as 'events data'.

The IPA removes the necessity for local authorities to seek the approval of a Justice of the Peace when seeking to acquire communications data. All such applications must now be processed through the National Anti-Fraud Network ("NAFN") and will be considered for approval by the independent Office of Communication Data Authorisation ("OCDA"). The transfer of applications between local authorities, NAFN and OCDA is conducted electronically.

All such applications will be considered by the Assistant Director (Legal and Democratic Services) before it is formally processed through the NAFN and considered for approval by the OCDA - in accordance with Section 2 of the Communications Data, Code of Practice (Communications Data Acquisition and Disclosure), published on the Home Office website.

L. Data Assurance/Retention

The Council will ensure that all information and material obtained through surveillance and all copies, extracts or summaries must be stored securely to minimise the risk of theft or loss. Only the officer who made the application (or their Team Lead) and the Authorising Officer with authority should be able to access the information.

All evidence obtained should be documented on a RIPA data retention form (Form RIP 9) and a copy must be sent to the Assistant Director, Corporate and Contracted Services on cancellation of the application.

The Council has the following in place:

(a) A suite of information security policies, records management policies and a GDPR/DPA Policy;
(b) implementation of the appropriate technical and organisational controls and measures to ensure an appropriate level of security; and
(c) physical security to protect all Council premises where the information is stored (electronically or manually) or can be accessed.

The information obtained through surveillance, and all copies, extracts and summaries, which contain such material, should be scheduled for deletion or destruction and securely destroyed as soon as they are no longer needed for the authorised purpose(s). If such information is retained, it should be reviewed at appropriate intervals to confirm that the justification for its retention is still valid, this will be monitored through the RIPA Central Register.

Records shall be maintained for a period of at 7 years in accordance with Council's Retention Schedule Policy (DBC400), following which, they shall be securely destroyed in accordance with that aforesaid retention policy.

M. Concluding Remarks of the Assistant Director (Legal and Democratic Services)

1. Where there is an interference with the right to respect for private life and family guaranteed under Article 8 of the European Convention on Human Rights, and where there is no other source of lawful authority for the interference, or if it is held not to be necessary or proportionate to the circumstances, the consequences of not obtaining or following the correct authorisation procedure set out in RIPA and this document, may be that the action (and the evidence obtained) will be held to be unlawful by the Courts pursuant to Section 6 of the Human Rights Act 1998.

2. Obtaining an authorisation under RIPA and following this document, will ensure, therefore, that the action is carried out in accordance with the law and subject to stringent safeguards against abuse of anyone's human rights.

3. Authorising Officers must direct their minds to the application every time they are asked to sign a form. They must never sign or rubber stamp forms without thinking about their personal and the Council's responsibilities.

4. Any boxes not needed on the form(s) must be clearly marked as being 'NOT APPLICABLE', 'N/A' or a line put through the same. Great care must also be taken to ensure accurate information is used and is inserted in the correct boxes. Reasons for any refusal of an application must also be kept on the form and the form retained for future inspections.

5. For further advice and assistance on RIPA, please contact the Council's Assistant Director (Legal and Democratic Services) who is also the Council's Monitoring Officer.

Appendix 1 – List of Authorising Officer Posts

	Service area
Chief Executive – (only where confidential information is likely to be acquired, or where it is proposed to use juveniles or vulnerable persons as covert human intelligence sources) or, in the absence of the Chief Executive, the person deputising for him/her	**All**
Chief Finance Officer	**Environmental Crime, Anti-social behavior and licensing , Corporate Fraud Planning Enforcement**
Strategic Director (Place)	**Environmental Crime, Anti-social behavior and licensing , Corporate Fraud Planning Enforcement**

IMPORTANT NOTES

A. Only the Chief Executive or the person deputising for him/her are authorised to sign forms relating to Juvenile Sources and Vulnerable Individuals (see Section F).

B. If a Chief Officer wishes to add, delete or substitute a post, s/he must refer such request to the Assistant Director (Legal and Democratic Services) for consideration, as necessary.

C. If in doubt, ask the Assistant Director (Legal and Democratic Services) BEFORE any directed surveillance and/or CHIS is authorised, renewed, rejected or cancelled.

APPENDIX 2

RIPA FLOW CHART

Requesting Officer ('The Applicant') must:

- Read the Corporate Policy & Procedures Document and be aware of any other guidance issued by the Assistant Director (Legal and Democratic Services).
- Determine that directed surveillance and/or a CHIS is required.
- Assess whether authorisation will be **in accordance with the law**
- Assess whether authorisation is **necessary** under RIPA and whether it could be done overtly.
- Consider whether surveillance will be **proportionate**
- If authorisation is approved – review regularly

If a less intrusive option is available and practicable **use that option!**

If authorisation is necessary and proportionate, prepare and submit an approved form to the Authorising Officer

Authorising Officer must:

- Consider in detail whether all options have been duly considered, including the Corporate Policy & Procedures Document and any other guidance issued by the Assistant Director (Legal and Democratic Services).
- Consider whether surveillance is considered by him/her to be **necessary** and **proportionate** and, if directed surveillance, that it meets the **crime threshold test**
- Authorise only if an overt or less intrusive option is not practicable and set review date
- Request the Assistant Director (Corporate and Contracted Services) to obtain

The Applicant must:
REVIEW REGULARLY (complete Review Form RIP4) and submit to Authorising Officer on date set

Authorising Officer must: If surveillance is still necessary and proportionate

- Review authorisation
- Set an appropriate further review date

The Applicant must:
If operation is no longer necessary or proportionate, complete **CANCELLATION FORM** RIP 3 and submit to Authorising Officer

Authorising Officer must:
Cancel authorisation when it is no longer necessary or proportionate to need the same

ESSENTIAL
Send all authorisations, reviews, renewals, cancellations and rejections to the Assistant Director (Corporate and Contracted Services)) within 1 week of the relevant event

NB: If in doubt, ask the Assistant Director (Legal and Democratic Services) BEFORE any directed surveillance and/or CHIS is authorised, renewed, cancelled or rejected.

Appendix 3

RIPA forms

- Form RIP 1 **Authorisation** Directed Surveillance
- Form RIP 2 **Renewal** of a Directed Surveillance Authorisation
- Form RIP 3 **Cancellation** of a Directed Surveillance Authorisation
- Form RIP 4 **Review** a Directed Surveillance Authorisation
- Form RIP 5 **Application** for Authorisation of the conduct or use of a Covert Human Intelliegence Source (CHIS)
- Form RIP 6 **Application** for Renewal of a CHIS
- Form RIP 7 **Cancellation** of an Authorisation for the use or conduct of a CHIS
- Form RIP 8 **Review** of a CHIS Authorisation
- Form RIP 9 Data retention form